Masterscriptie

Communicatie en Organisatie

Sharing is caring?

Kwalitatief onderzoek naar de manier waarop zorginstellingen hun interne communicatie over privacybescherming en informatiebeveiliging inrichten om te kunnen opereren conform de nieuwe privacywet- en regelgeving

Bronnen: NRC en nu.nl (2016)

Student: Renske Swarts

Studentnummer: 5622328

E-mail: renskeswarts@gmail.com

Docent: dr. Hanny den Ouden

Tweede lezer: dr. Ingeborg van der Geest

Stagebegeleiders Winkelman en Van Hessen:

Michel van Schie

Sharon McIntosh

Datum: 16-01-2017

Universiteit Utrecht

Managementsamenvatting

Individuen en organisaties leven volgens het principe ‘sharing is caring’. Het liefst delen we zoveel mogelijk gegevens met elkaar. Individuen om elkaar op de hoogte te stellen van hun dagelijks leven; organisaties om beter in te spelen op de klant. Dit gaat ten koste van de privacy van individuen. Daarom heeft de overheid de wetgeving rondom privacy en informatiebeveiliging aangepast. Er komen strengere regels en er komt meer verantwoordelijkheid voor organisaties. Met deze regels maken we de overstap van het principe ‘sharing is caring’ naar het principe ‘care before you share’.

In dit onderzoek staat dit tweede principe centraal en wordt gekeken hoe interne communicatie een rol kan spelen bij de invulling van de privacywet- en regelgeving rekening houdend met nieuwe aspecten als de meldplicht datalekken en de Algemene Europese Verordening voor de Gegevensbescherming. Om beter zicht te krijgen op dit thema is verdiept in de zorgsector waar ook bijzondere persoonsgegevens een rol spelen.

Het doel van dit onderzoek was om richtlijnen te creëren voor de zorgsector om hun interne communicatie rondom privacybescherming en informatiebeveiliging in te kunnen richten. De hoofdvraag die hierbij hoorde was: *Hoe kunnen zorginstellingen hun interne communicatie rondom privacybescherming en informatiebeveiliging zo inrichten dat zij conform de huidige wet- en regelgeving opereren?*

Om een antwoord te formuleren op deze hoofdvraag is eerst in het theoretisch kader verder onderzocht wat de algemene privacywet- en regelgeving inhoudt en welke rol communicatie bij de invulling van deze wetgeving kan vervullen. Vervolgens zijn twee deelstudies gedaan.

In de eerste deelstudie is een documentanalyse uitgevoerd op de bestaande documenten over de privacywet- en regelgeving en is gekeken welke aansluitingen er waren met communicatie. Uit deze bestaande documenten zijn communicatierichtlijnen afgeleid welke een basis vormden voor de interviews in deelstudie 2. Deze communicatierichtlijnen geven bovendien een globaal antwoord op de hoofdvraag, omdat zij op basis van de huidige wet- en regelgeving geformuleerd zijn. De geformuleerde communicatierichtlijnen luidden als volgt:

1. Actieve betrokkenheid van het bestuur
2. Privacy krijgt een hoge prioriteit in de organisatie
3. Er is een risico-inventarisatie gedaan
4. De risico’s van een beveiligingsissue zijn in beeld bij het bestuur
5. Er is op basis van de risico-inventarisatie een beleidsdocument informatiebeveiliging opgesteld
6. Er wordt regelmatig gecommuniceerd over het beleidsdocument informatiebeveiliging
7. Er wordt gewerkt aan het verhogen van beveiligingsbewustzijn in de organisatie
8. Er zijn duidelijke procedures aanwezig voor het behandelen van beveiligingsincidenten
9. Er wordt regelmatig over deze procedures gecommuniceerd
10. De gekozen maatregelen worden regelmatig geëvalueerd
11. Het beleid wordt na evaluatie indien nodig aangepast

Deze richtlijnen zijn vrij globaal. Om beter zicht te krijgen op hoe invulling gegeven wordt aan het interne communicatiebeleid rondom privacybescherming en informatiebeveiliging zijn ter aanvulling interviews gehouden met experts en functionarissen gegevensbescherming van zorginstellingen. Deze twee groepen gaven aan op welke manier zij invulling gaven aan de geformuleerde communicatierichtlijnen uit deelstudie 1. Met behulp van deze antwoorden kregen de communicatierichtlijnen uit deelstudie 1 meer lading en kon er een inhoudelijker antwoord geformuleerd worden op de hoofdvraag. Ook bleek tijdens de interviews dat een aantal richtlijnen minder toepasbaar waren of eenvoudig samengevoegd konden worden. Dit leidde tot een aantal communicatieadviezen voor de zorgsector. Deze uitkomsten vormden tevens het antwoord op de hoofdvraag en worden hieronder genoemd.

1. Zorg voor actieve betrokkenheid van het bestuur

Een zorginstelling kan actieve betrokkenheid realiseren door een bestuurslid portefeuillehouder van privacy te maken of door leden van de bestuursstaf onderdeel te maken van het privacyteam. Andere mogelijkheden zijn om het bestuur verantwoordelijk te maken voor meldingen om op deze manier incidenten bespreekbaar te maken op bestuursniveau en risico’s van beveiligingsincidenten scherp in beeld te houden.

2. Zorg voor prioriteit van privacy

Om volgens de huidige privacywet- en regelgeving te kunnen opereren moet een zorginstelling aan kunnen tonen dat privacy hoge prioriteit heeft. Dit kan een zorginstelling bijvoorbeeld doen door een privacywerkgroep of een goed opgeleide (extra) functionaris voor de gegevensbescherming aan te stellen, door privacy op de agenda te zetten van vergaderingen, door budget vrij te maken voor privacy of door het onderdeel te maken van het functioneren van de medewerker.

3. Breng risico's van beveiligingsissues in kaart en stel op basis daarvan een informatiebeveiligingsbeleid op

Een zorginstelling kan risico's in kaart brengen door een Privacy Impact Assessment te doen of privacynulmeting afhankelijk van het stadium waarin de instelling zich bevindt. Een Privacy Impact Assessment is uitgebreider dan een nulmeting, waardoor een instelling aan meer eisen moet voldoen. Op basis van deze risicoanalyse kan een zorginstelling vervolgens een informatiebeveiligingsbeleid opstellen, waarbij de hoogste prioriteit uitgaat naar de hoogste risico's en hoe deze worden aangepakt. Belangrijk bij dit punt is dat er niet alleen gelet wordt op de risico's op een boete of op risico's van technische aard, maar dat ook organisatorische risico's worden meegenomen, zoals mogelijke reputatieschade en het verlies van patiëntvertrouwen.

4. Communiceer over het informatiebeveiligingsbeleid en werk aan het verhogen van beveiligingsbewustzijn

Een zorginstelling kan gebruik maken van verschillende communicatiemiddelen om te communiceren over het informatiebeveiligingsbeleid. Zo kan een zorginstelling voorlichting geven, presentaties houden of een brochure maken, waarin uitleg gegeven wordt over het informatiebeveiligingsbeleid. Op deze manier kan kennis over het informatiebeveiligingsbeleid en de bijbehorende regels gemakkelijk verspreid worden over de organisatie. Voor het verhogen van beveiligingsbewustzijn moet een zorginstelling nog een stapje verder gaan. Hiervoor is namelijk ook de motivatie van medewerkers nodig om volgens de nieuwe wet- en regelgeving te handelen. Dit betekent dat het simpelweg presenteren van het beleid op verschillende manieren niet voldoende is. Het is ook nodig om medewerkers te trainen in de nieuwe wet- en regelgeving en bewustwordingscampagnes in te zetten. Ook gebouwrondes kunnen helpen bij het creëren van bewustwording van medewerkers, omdat ze op deze manier zien dat de regels gehandhaafd worden. In een grote organisatie is het wellicht handig een ambassadeurssessie te organiseren en van elke afdeling iemand als privacyambassadeur in te zetten. Zo hoeft de organisatie niet elke medewerker apart te informeren, maar kunnen de privacyambassadeurs het onderwerp onder de aandacht brengen en houden op hun afdeling. Herhaling en variatie zijn sleutelwoorden bij communicatie. Niet iedereen neemt informatie op dezelfde manier tot zich, dus hou hier rekening mee bij het organiseren van de interne communicatie.

5. Stel duidelijke procedures op voor het behandelen van beveiligingsincidenten en communiceer hierover

Om beveiligingsincidenten te behandelen moeten in een zorginstelling duidelijke procedures aanwezig zijn. Zo moet bijvoorbeeld duidelijk zijn wie waarvoor verantwoordelijk is en wanneer er een melding moet worden gedaan bij de Autoriteit Persoonsgegevens. Daarom is het belangrijk om dit vast te leggen en duidelijk te communiceren naar de organisatie. Dit kan op dezelfde manier als gecommuniceerd wordt over het informatiebeveiligingsbeleid. Zorg in ieder geval dat medewerkers weten waar ze een melding kunnen doen en betrek medewerkers ook in het proces door terug te koppelen aan hen wat er met de meldingen gebeurd is.

6. Evalueer regelmatig het informatiebeveiligingsbeleid en pas het beleid indien nodig aan

Om het informatiebeveiligingsbeleid up-to-date te houden is het van belang continu te kijken naar verbeterpunten in het beleid. Zeker met de komst van de Algemene Europese Verordening is het van belang de privacywet- en regelgeving continu te checken en te kijken of er nog steeds in lijn met deze wetgeving gehandeld wordt.

Inhoudsopgave

1. Inleiding

Als individu heb je het recht om te weten welke gegevens over jou worden verzameld en waarom. Dit staat beschreven in de grondwet over privacy[1]. Vroeger kon je voor privacy je gordijnen dichtdoen of een deur sluiten en dan kon je met een gerust hart over gevoelige onderwerpen praten. De afgelopen jaren heeft onze samenleving een enorme digitale groei doorgemaakt, waardoor het sluiten van een deur niet meer voldoende is om privacy te garanderen. Inmiddels leven we steeds meer volgens het principe 'sharing is caring'. Door even op Facebook te zitten, een zoekopdracht in te voeren op Google of een bestelling te doen op bol.com geef je je gegevens aan organisaties. Organisaties verzamelen deze gegevens om meer informatie over hun klanten te krijgen. Dit zorgt voor groeiende databases. De databases zijn inmiddels zo groot dat het onmogelijk is om als individu te weten wat organisaties allemaal over jou verzamelen. Sterker nog, ook voor organisaties is het een enorme klus om dit inzichtelijk te maken[2].

Dit was aanleiding voor de overheid om de wet- en regelgeving rondom privacy aan te passen. Uit onderzoek blijkt echter dat het lastig is voor organisaties om aan deze nieuwe privacywet- en regelgeving te voldoen. Uit een Privacy Governance Onderzoek van PWC (2015) blijkt bijvoorbeeld dat er nog geen sprake is van volwassenheid van privacybeheersing binnen Nederlandse organisaties. Dit onderzoek is uitgevoerd onder 93 organisaties in verschillende sectoren. In 2015 gaf 16% aan voorbereid te zijn op de nieuwe privacy wet- en regelgeving en dacht slechts 35% van de deelnemers dat de eigen organisatie gekwalificeerd was om zorgvuldig om te gaan met persoonsgegevens. Bedrijven worstelen dus met het invullen van de nieuwe privacywet- en regelgeving.

Het invullen van de nieuwe privacywet- en regelgeving houdt in dat de wetten en regels vertaald moeten worden naar werkbare richtlijnen voor medewerkers. Dit maakt het invullen van de nieuwe privacywet- en regelgeving tot een organisatorisch vraagstuk. Interne communicatie speelt bij het doorvoeren van veranderingen in het privacybeleid een belangrijke rol (Clampitt, 2013). Bij dit onderwerp speelt het een bijzondere rol, omdat iedereen op alle niveaus in de organisatie zich volgens de nieuwe privacywet- en regelgeving moet gaan gedragen. Ook medewerkers zullen dus aanpassingen moeten doen in hun werkproces om aan deze nieuwe wet- en regelgeving te voldoen. De centrale vraag voor organisaties hierbij is hoe zij met behulp van interne communicatie ervoor kunnen zorgen dat zij binnen de kaders van de wet opereren.

Om meer zicht te krijgen op dit vraagstuk wordt in dit onderzoek gekeken naar de invulling van de nieuwe privacywet- en regelgeving in de zorgsector. Hierbij hoort de volgende hoofdvraag:

Hoe kunnen zorginstellingen hun interne communicatie rondom privacybescherming en informatiebeveiliging zo inrichten dat zij conform de huidige wet- en regelgeving opereren?

De keuze voor de zorgsector wordt verder toegelicht in hoofdstuk 2.3. De huidige wet- en regelgeving en de bijbehorende begrippen zullen in het theoretisch kader verder worden uitgelegd. Vervolgens zal gekeken worden welke communicatierichtlijnen afgeleid kunnen worden van deze algemene wet- en regelgeving in hoofdstuk 3. In hoofdstuk 4 zal gekeken worden hoe experts en functionarissen voor de gegevensbescherming van zorginstellingen op dit moment invulling geven aan de wet- en regelgeving om ten slotte adviezen te geven voor de interne communicatie van zorginstellingen rondom privacybescherming en informatiebeveiliging. Met deze adviezen kunnen we zorginstellingen helpen om van het principe 'sharing is caring' over te gaan naar het principe 'care before you share', waarbij rekening gehouden wordt met de privacy van individuen en persoonsgegevens goed beschermd worden alvorens zij worden gedeeld.

[1] Artikel 10 Privacy, Grondwet voor het Koninkrijk der Nederlanden (2008) Hoofdstuk 1: Grondrechten

[2] Dit wordt duidelijk in het boek *je hebt wél iets te verbergen* van onderzoeksjournalisten Maurits Martijn en Dimitri Tokmetzis

2. Theoretisch kader

De privacywet- en regelgeving bestaat uit verschillende elementen, zoals de Wet bescherming persoonsgegevens, de Wet meldplicht datalekken en de Algemene Europese Verordening voor de gegevensbescherming. De Wet bescherming persoonsgegevens en de Wet meldplicht datalekken kunnen gezien worden als voorwaarden om het recht op privacy van het individu te kunnen garanderen. Er zal daarom eerst ingegaan worden op wat er in de grondwet over privacy beschreven staat, waarna specifieker ingegaan zal worden op de centrale begrippen uit de Wet meldplicht datalekken en de Wet bescherming persoonsgegevens. In dit hoofdstuk zal duidelijk worden hoe de definitie van privacy zich in de loop der jaren heeft ontwikkeld en hoe er invulling wordt gegeven aan het garanderen van privacy met behulp van wet- en regelgeving over informatiebeveiliging en de bescherming van persoonsgegevens. Vervolgens zal in dit hoofdstuk de interne communicatie rondom deze wet- en regelgeving in organisaties aan bod komen, waarna zal worden ingezoomd op de zorgsector.

2.1 De uitbreiding van privacywet- en regelgeving

2.1.1 Ontwikkelingen van definitie van privacy

In 1890 kwamen Warren en Brandeis met de definitie van privacy als 'the right to be let alone' oftewel het recht om met rust gelaten te worden.

Bijna een eeuw later kwam de definitie van privacy als informationeel zelfbeschikkingsrecht tot stand (Westin, 1968). Dit hield in dat individuen het recht hebben om zelf te beslissen wanneer, hoe en in welke mate persoonlijke informatie met anderen wordt gedeeld. In de huidige eeuw kwamen hier nog een aantal definities bij zoals: 'vrijheid van onredelijke beperkingen om je eigen identiteit te construeren' van Agre en Rotenberg (2001).

Waar privacy in de 19e eeuw nog bestond uit met rust gelaten worden wanneer je dit wilde, is dit in de huidige maatschappij veranderd naar ervoor zorgen dat je de mogelijkheid hebt om je eigen identiteit te construeren. Jij hoort te bepalen welke informatie je met wie deelt en waarom. In artikel 10 van de grondwet over privacy staat beschreven (Grondwet voor het Koninkrijk der Nederlanden, 2008)[3]:

1. Iedereen heeft recht op rust en privacy. In de wet kunnen uitzonderingen staan. In de wet kan ook staan dat iemand anders uitzonderingen mag maken.

2. De overheid mag persoonlijke gegevens van iemand niet zomaar gebruiken.

3. Iedereen heeft er recht op te zien wat er over hem is vastgelegd. En kan gegevens laten veranderen als ze niet juist zijn.

De opkomst van technologie en sociale media zorgen voor een grote uitwisseling van data. Dit maakt het voor individuen lastig om zicht te krijgen op welke informatie organisaties over hen hebben en hoe zij met deze informatie omgaan (Martijn & Tokmetzis, 2016). Neem bijvoorbeeld Google en Facebook die over een oneindig grote database beschikken om hun website aan te passen aan de bezoeker, maar ook aan de overheid die data over jou verzamelt. Het is daarom niet meer alleen de verantwoordelijkheid van het individu om privacy te waarborgen, maar ook de verantwoordelijkheid van organisaties.

Zoals in de grondwet al wordt aangegeven mag de overheid niet zomaar persoonlijke gegevens van jou gebruiken. Dit geldt sinds 2001 ook voor organisaties toen de Wet bescherming persoonsgegevens in het leven is geroepen. Inmiddels wordt er ook op toegezien dat organisaties zorgvuldig omgaan met persoonsgegevens en zijn er consequenties verbonden aan het niet zorgvuldig omgaan met persoonsgegevens met de Wet meldplicht datalekken die in 2016 is ingevoerd. Deze Meldplicht kan in combinatie met de Wbp gezien worden als voorbode van de Algemene Europese Verordening, die vanaf 2018 handhaafbaar wordt.

[3] Artikel 10 Privacy, Grondwet voor het Koninkrijk der Nederlanden (2008) Hoofdstuk 1: Grondrechten

2.1.2 Op weg naar de Algemene Verordening voor de Gegevensbescherming

Voordat ingegaan zal worden op de veranderingen die de Algemene Verordening voor de Gegevensbescherming tot gevolg heeft voor organisaties, zal hieronder eerst toelichting gegeven worden van de belangrijkste ontwikkelingen in de privacywet- en regelgeving van de afgelopen jaren. De belangrijkste bepalingen uit de Wet bescherming persoonsgegevens zijn de volgende:

- Persoonsgegevens mogen alleen in overeenstemming met de wet en op een behoorlijke en zorgvuldige manier worden verwerkt.

- Persoonsgegevens mogen alleen voor welbepaalde, vooraf uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld. En vervolgens alleen verder worden verwerkt voor doeleinden die daarmee verenigbaar zijn.

- Degene van wie persoonsgegevens worden verwerkt (de betrokkene genoemd), moet ten minste op de hoogte zijn van de identiteit van de organisatie of persoon die deze persoonsgegevens verwerkt (de zogeheten verantwoordelijke) en van het doel van de gegevensverwerking.

- De gegevensverwerkingen moeten op een passende manier worden beveiligd. Voor bijzondere gegevens, zoals over ras, gezondheid en geloofsovertuiging, gelden extra strenge regels (Autoriteit Persoonsgegevens, 2016).

In de Wet bescherming persoonsgegevens staat duidelijk beschreven wat organisaties wel en niet mogen tijdens hun verzameling van persoonsgegevens en wordt ook duidelijk dat organisaties verantwoordelijk zijn voor het beschermen van persoonsgegevens door persoonsgegevens op een passende manier te beveiligen. Een organisatie moet zowel technische als organisatorische maatregelen nemen in de beveiliging van persoonsgegevens (Autoriteit Persoonsgegevens, 2015).

Om meer verantwoordelijkheid te geven aan organisaties met betrekking tot het beschermen van persoonsgegevens is op 1 januari 2016 de meldplicht datalekken in het leven geroepen. Deze meldplicht houdt in dat organisaties direct een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij de bescherming van persoonsgegevens niet kunnen garanderen en een boete riskeren wanneer zij dit niet doen (Autoriteit Persoonsgegevens, 2016). Er wordt gesproken van een datalek wanneer er inbreuk is op de beveiliging van persoonsgegevens (zoals bedoeld in artikel 13 van de Wet bescherming persoonsgegevens). Bij een datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking (Autoriteit Persoonsgegevens, 2015). Een datalek moet worden gemeld aan de Autoriteit Persoonsgegevens als het leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens.[4] Het datalek moet daarnaast ook worden gemeld aan de betrokkene indien het waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer.[5]

De komst van de meldplicht datalekken heeft consequenties voor organisaties en hun beleid. De wet- en regelgeving rondom privacy is de afgelopen jaren enorm uitgebreid en er komt meer druk op organisaties om te voldoen aan deze wet- en regelgeving. Vanaf 25 mei 2018 is de Algemene Verordening voor de Gegevensbescherming (AVG) van kracht. Deze is rechtstreeks van toepassing in alle EU-lidstaten. Er geldt vanaf die datum dus nog maar één privacywet in Europa in plaats van verschillende nationale wetten (AVG, 2016). De meldplicht datalekken kan gezien worden als een opstapje naar de AVG. Met behulp van de meldplicht datalekken kunnen organisaties alvast wennen aan het krijgen van meer verantwoordelijkheden op het gebied van privacy, waardoor de stap naar de AVG minder groot is.

Er wordt in de AVG naast op meer verantwoordelijkheid voor de organisatie, ook meer nadruk gelegd op *accountability* van organisaties. Dit betekent dat organisaties moeten kunnen aantonen dat zij zich aan de wet houden. Organisaties krijgen documentatieplicht. Zij moeten met documenten kunnen aantonen dat zij de juiste organisatorische en technische maatregelen hebben genomen om aan de AVG te voldoen (AVG, 2016). De functionaris voor de gegevensbescherming (FG) is de persoon in de organisatie die erop toeziet

[4] artikel 34a, eerste lid, Wbp
[5] artikel 34a, tweede lid, Wbp

dat er een passend beleid wordt opgesteld dat voldoet aan de privacywet- en regelgeving (Autoriteit Persoonsgegevens, 2017). Een FG moet onafhankelijk van de organisatie zijn werkzaamheden kunnen verrichten en moet bevoegd zijn om ruimtes te betreden, zaken te onderzoeken en inzage te vragen. Een FG kent ontslagbescherming. Ook moet een FG voldoende kennis hebben van de organisatie en de privacywetgeving (Autoriteit Persoonsgegevens, 2017). De taken van een FG bestaan uit toezicht houden, inventarisaties van gegevensverwerkingen maken, meldingen van gegevensverwerkingen bijhouden, vragen en klachten van mensen binnen en buiten de organisatie afhandelen, interne regelingen ontwikkelen, adviseren over technologie en beveiliging en input leveren bij het opstellen of aanpassen van een gedragscode. Een FG handelt dus niet in het belang van de organisatie maar in het belang van de samenleving.

De normen die gesteld worden aan de praktijk worden steeds strenger, zoals ook te zien is in de NEN-7510[6] en ISO-27001[7]. Alle reden dus voor organisaties om technische en organisatorische maatregelen te nemen zodat ze kunnen voldoen aan de wet- en regelgeving. Deze technische en organisatorische maatregelen worden door organisaties vormgegeven in een informatiebeveiligingsbeleid. Deze term wordt overkoepelend gebruikt voor het op zo'n manier inrichten van het beleid dat wordt voldaan aan privacywet- en regelgeving.

2.1.3 Informatiebeveiliging

Op het eerste gezicht lijkt informatiebeveiliging een vrij technische term. Informatiebeveiliging omvat het geheel aan maatregelen waarmee organisaties hun informatie beveiligen (CBP, 2013). [8] Het gaat daarbij om alle informatie die de organisatie verwerkt, zowel digitaal als niet-digitaal. Ook als gekeken wordt naar de vier aspecten van informatiebeveiliging die onderscheiden worden in het vakgebied dan lijkt informatiebeveiliging vooral een technisch karakter te hebben:

- Beschikbaarheid
  Beschikbaarheid betreft het waarborgen dat geautoriseerde gebruikers op de juiste momenten toegang hebben tot informatie en aanverwante bedrijfsmiddelen (informatiesystemen).
- Integriteit
  Integriteit betreft het waarborgen van de juistheid, tijdigheid (actualiteit) en volledigheid van informatie en de verwerking ervan.
- Vertrouwelijkheid
  Met vertrouwelijkheid wordt gedoeld op het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe zijn geautoriseerd.
- Controleerbaarheid
  Controleerbaarheid betreft de mogelijkheid om met voldoende zekerheid te kunnen vaststellen of wordt voldaan aan de eisen ten aanzien van beschikbaarheid, integriteit en vertrouwelijkheid.

Toch als verder gekeken wordt naar de richtsnoeren voor informatiebeveiliging die zijn opgesteld door de Autoriteit Persoonsgegevens, lijkt er ook een belangrijke rol weggelegd voor de organisatorische kant. Zo moet op basis van risicoanalyse gekeken worden welke gevolgen incidenten hebben voor de organisatie en hoe deze risico's in te perken zijn. Op het organisatorische vlak is een belangrijke rol weggelegd voor communicatie. Communicatie kan er namelijk niet alleen voor zorgen dat mensen weten van de regels en de wet, maar kan ook een bijdrage leveren aan de bewustwording van medewerkers om goed met persoonsgegevens om te gaan. De beveiliging van persoonsgegevens moet binnen de organisatie daarnaast een blijvend punt van aandacht zijn (Autoriteit Persoonsgegevens, 2016). Ook in het aandacht geven aan het onderwerp privacy kan communicatie een rol spelen.

2.2 Communiceren van privacywet- en regelgeving in organisaties

Voor bedrijven is het een grote stap om aan de privacywet- en regelgeving te voldoen. Naast een aantal beveiligingsmaatregelen waaraan een bedrijf moet voldoen, moet er ook veel veranderen op organisatorisch gebied (Autoriteit Persoonsgegevens, 2015). Er moet duidelijk worden wie verantwoordelijk is voor welk

[6] Voor de inhoud van de NEN-7510-norm zie https://www.werkenmetnen7510.nl/publicaties/nen-7510-2011
[7] Voor de inhoud van de ISO-27001 zie http://www.slinfo.una.ac.cr/documentos/EIF402/ISO27001.pdf

[8] Het College Bescherming Persoonsgegevens heet sinds 1 januari 2016 officieel Autoriteit Persoonsgegevens. Indien verwezen wordt naar documenten van voor de naamwisseling wordt CBP gebruikt, maar dit is dus dezelfde instantie als Autoriteit Persoonsgegevens.

onderdeel van dataprotectie en het melden hiervan en ook moeten alle medewerkers op de hoogte zijn van wat de wet voor hun bedrijf betekent. Vervolgens moet er ook een zeker bewustzijn aangebracht worden bij medewerkers en er moet een crisisbeleid zijn voor als er een datalek komt (CBP, 2013). Enkel als hier protocollen voor bestaan en er goed is omgesprongen met de eigen verantwoordelijkheid, is de Autoriteit Persoonsgegevens tevreden.

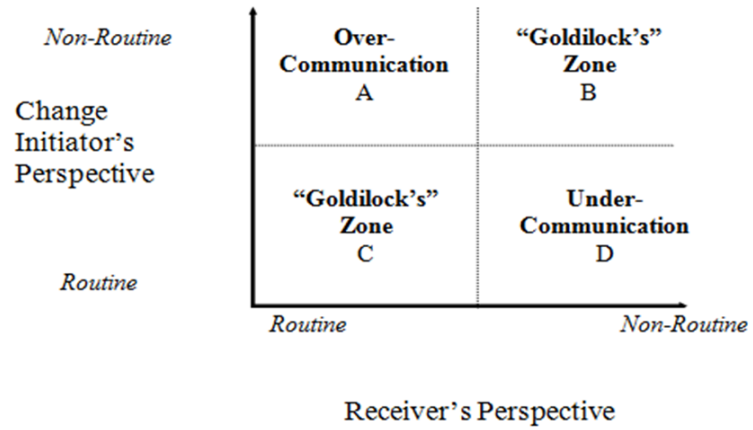
Uit onderzoek is gebleken dat 80% van de datalekken door foutief handelen van medewerkers ontstaat (Verizon, 2016). Hierdoor wordt het nog belangrijker om medewerkers mee te nemen in het nieuwe beleid en weerstanden tegen te gaan. Communicatie kan hier een belangrijke rol in spelen. In dit hoofdstuk zal duidelijk worden waar een organisatie rekening mee moet houden bij een verandering in beleid en hoe communicatie een rol speelt bij het invoeren van nieuw beleid in organisaties. De focus ligt op hoe communicatie een rol kan spelen bij het goed doorvoeren van de nieuwe privacywet- en regelgeving en het daarmee beperken van risico's op een beveiligingsissue en dus niet op de invulling van crisiscommunicatie wanneer er een beveiligingsincident plaatsvindt.

2.2.1 Verandering van beleid: waar moet een organisatie rekening mee houden?

Soort verandering: routinematig of non-routinematig

Veranderingen kunnen worden beschreven op een continuüm van routinematig naar non-routinematig (Clampitt, 2013). Niet iedereen in de organisatie heeft hetzelfde perspectief bij een verandering. Er kan hierin een verschil zitten tussen degene die de verandering initieert en degene die de verandering moet doorvoeren. Er moet dus een duidelijke afweging gemaakt worden in de hoeveelheid informatie die gecommuniceerd wordt. Te weinig informatie kan leiden tot onzekerheid bij werknemers, waar te veel informatie juist weer kan leiden tot onduidelijkheid over wat wel en niet klopt.

Volgens Clampitt (2013) hangt de hoeveelheid informatie af van twee vragen: Heeft de initiatiefnemer al eerder eenzelfde soort verandering meegemaakt? En/of hebben de werknemers van de organisatie al eerder eenzelfde soort verandering meegemaakt? In Figuur 1 is te zien hoe deze vragen samenhangen met de communicatie die per situatie nodig is. Is de situatie bekend bij de initiatiefnemer (routine), maar onbekend bij de werknemers (non-routine), dan is het gevaar dat de initiatiefnemer te weinig communiceert (*undercommunication*). Zijn tactiek en alle informatie zit al langere tijd in zijn hoofd, maar dat betekent niet dat alles ook voor de werknemers zo vanzelfsprekend is. Is de situatie onbekend bij de initiatiefnemer (non-routine), maar wel bekend bij de werknemers (routine), dan is het gevaar dat de initiatiefnemer juist te veel communiceert (*overcommunication*). Werknemers weten al hoe ze in moeten spelen op de situatie, waardoor te veel (onnodige) informatie alleen maar tot verwarring en irritatie kan leiden. De ideale situaties zijn wanneer de verandering voor zowel initiatiefnemers als werknemers bekend of onbekend is (Goldilock's Zone). Voor routinematige veranderingen is 'simpele' informatieoverdracht voldoende, maar voor non-routinematige veranderingen is meer communicatie nodig (p. 236 - 237).



Figuur 1: 'Selecting the degree of information' (Clampitt, 2013, p236)

In het geval van communiceren over informatiebeveiliging en de meldplicht datalekken is het de vraag of het om een routinematige of een non-routinematige verandering gaat. Dit kan per organisatie verschillen: voor de één kan iets een routinematige verandering zijn, waar dit voor de ander een non-routinematige verandering is. De

aanwezige communicatiecultuur kan als maatstaf genomen worden om te kijken of een verandering routinematig of non-routinematig is.

Als er in een bedrijf al veel gedaan wordt aan dataprotectie en het bedrijf privacy hoog in het vaandel heeft staan, dan kan er sprake zijn van een routinematige verandering. Er komt dan enkel een nieuwe wet bij met de Wet meldplicht datalekken, die uitgelegd moet worden aan medewerkers. Deze zal in hun handelen niet veel veranderen, omdat het belang van privacy al duidelijk is bij de medewerker. Als er in een bedrijf echter niet duidelijk is wat gevoelige gegevens zijn en hoe hiermee omgegaan dient te worden, dan spreken we van een non-routinematige verandering. De communicatie moet afgestemd worden op het soort verandering.

Reacties en percepties van werknemers

De communicatie over de verandering kan met behulp van het model van Clampitt worden afgesteld op het niveau van de informatiebehoefte van de medewerkers. Met dit model kunnen echter geen uitspraken gedaan worden over de reacties van medewerkers op een verandering. Een verandering kan als vervelend worden ervaren voor werknemers, omdat ze hun huidige werkprocessen aan moeten passen. Bij informatiebeveiliging kan dit bijvoorbeeld gaan om het telkens automatisch uitloggen van de computer als een medewerker even weg loopt of het blokkeren van de mail voor het versturen van persoonsgegevens. Door Clampitt worden verschillende reactiemogelijkheden onderscheiden van werknemers bij een verandering: ontkenning (*denial and isolation*), woede (*anger*), onderhandeling (*bargaining*), depressie (*depression*) en acceptatie (*acceptance*) (Clampitt, 2013, p. 238).

Bovenstaande situatie zal vooral leiden tot ergernis, omdat het directe werkproces wordt verstoord. Zonder duidelijke uitleg van de noodzaak van deze maatregel zal het acceptatiegehalte laag liggen. Een manager zit nooit meteen op dezelfde golflengte als zijn medewerkers. De manager heeft een andere positie en heeft vaak met andere werkprocessen te maken, waardoor hij zich vaak in een ander deel van het proces bevindt dan de medewerkers (Clampitt, 2013, p. 240). Het is dan ook belangrijk voor een manager om zich flexibel op te stellen en rekening te houden met de verschillende reactiemogelijkheden, door voor iedere reactie een passend antwoord te hebben. Ook kan bovenstaande situatie ervoor zorgen dat medewerkers de opgestelde privacyregels niet gaan naleven, omdat hun werkproces dusdanig verstoord is en de regel niet door hen geaccepteerd wordt.

2.2.2 Rol van interne communicatie bij organisatieverandering

Volgens Vos en Schoemaker zijn problemen in de interne communicatie niet los te zien van de interne organisatie (2011). Het is dus van belang de interne communicatie op orde te hebben om problemen in de interne organisatie te voorkomen. Interne communicatie heeft verschillende functies:

- Het ondersteunen van het primaire proces
- Het bevorderen van betrokkenheid
- Het begeleiden van veranderingsprocessen

De belangrijkste functie bij het doorvoeren van de nieuwe privacywet- en regelgeving ligt bij het begeleiden van het veranderingsproces. Het overdragen van kennis van de nieuwe privacywet- en regelgeving helpt bij het vergroten van de betrokkenheid van medewerkers en de motivatie van medewerkers om zich aan de wet te houden.

Bij een verandering heeft een organisatie over het algemeen de volgende communicatiedoelstellingen:

- Medewerkers moeten op de hoogte zijn van de gewenste veranderingen en daarvan de achtergronden kennen (kennisdoelstellingen)
- Medewerkers moeten gemotiveerd zijn voor de veranderingen (houdingsdoelstellingen)
- Medewerkers moeten bereid zijn zich in te zetten om de verandering tot stand te brengen (gedragsintentie) (Vos & Schoemaker, 2011, p.116)

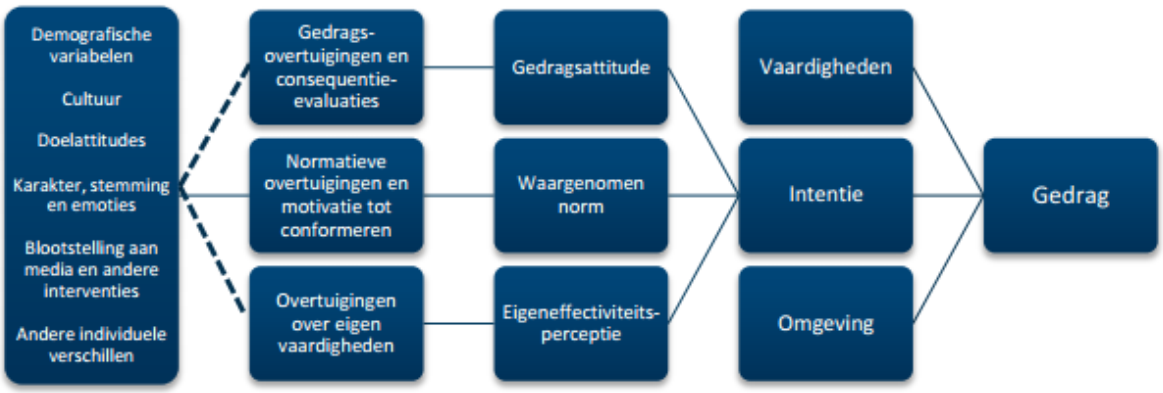
Deze drie doelstellingen zijn vergelijkbaar met de drie factoren die Winkelman (2015) aangeeft om een verandering te laten slagen: motivatie van medewerkers, een stimulerend klimaat en participatie. Motivatie ontstaat wanneer mensen zich persoonlijk betrokken voelen en zich identificeren met doelen van de organisatie (Vos & Schoemaker, 2011, p.95). In dit geval zal er motivatie van medewerkers moeten ontstaan om te conformeren aan de nieuwe privacywet- en regelgeving. Om de motivatie van medewerkers te krijgen is het van belang om een heldere koers, perspectief, progressie en betekenis te hebben. Dit kan weergegeven worden in een CEO story of via directie news flashes (Winkelman, 2015).

Een stimulerend klimaat kan ontstaan als er bijvoorbeeld een meldcultuur in de organisatie aanwezig is en/of een aanspreekcultuur. Aanstekelijk succes en samenwerking dragen bij aan een stimulerend klimaat. Door

het organiseren van events of het doen van postering kan een organisatie aanstekelijk succes en samenwerking realiseren. Ook moet er actieve participatie zijn van medewerkers. Betrokkenheid bij het privacythema kan helpen deze actieve participatie van medewerkers te realiseren. Onder betrokkenheid verstaan we de mate van identificatie van medewerkers met het werk en de organisatie (Vos & Schoemaker, 2011, p. 112). Het doen van trainingen of het geven van inspiratiesessies helpen bij het vergroten van betrokkenheid (Winkelman, 2015).

2.2.3 Communicatiedoelstellingen behalen bij verandering

Om de communicatiedoelstellingen die Vos en Schoemaker (2011) formuleren te behalen, zal een organisatie de houding en het gedrag van de medewerker positief moeten proberen te beïnvloeden. Dit kan met behulp van het *integrative model of behavioral prediction.* Dit model onderscheidt een aantal determinanten van beredeneerd gedrag (Fishbein & Azjen in Hoeken, Hornikx en Hustinx, 2012) (zie Figuur 2). Het gedrag van een persoon wordt volgens dit model bepaald door de gedragsintentie, de eigen vaardigheden en de omgevingsfactoren. De gedragsintentie wordt vervolgens weer bepaald door de attitude ten opzichte van het gedrag, de waargenomen norm ten opzichte van het gedrag en de eigeneffectiviteitsperceptie (ben ik in staat om het gedrag te vertonen).



Figuur 2: 'Integrative model of behavioral prediction' (Fishbein & Ajzen, 2011)

Zo wordt de intentie om volgens de privacywet- en regelgeving te handelen bepaald door de attitude dat het wenselijk is om volgens deze privacywet- en regelgeving te handelen, de gedachte dat anderen het wenselijk vinden om volgens de wet te handelen (waargenomen norm) en de perceptie of de medewerker in staat is om volgens de wet te handelen (eigeneffectiviteitsperceptie). Deze intentie bepaalt in combinatie met de eigen vaardigheden en omgevingsfactoren het uiteindelijke gedrag van een individu: gaat hij/zij volgens de wet handelen?

Om de communicatiedoelstellingen: op de hoogte zijn, gemotiveerd zijn en bereid zijn te behalen kan ingespeeld worden op bovengenoemde determinanten van gedrag. Deze bepalen namelijk of een persoon zijn gedrag zal veranderen of niet.

2.3 Communicatie van privacywet- en regelgeving in de zorgsector

In de zorgsector is de NEN-7510 opgesteld, waarin de privacywet- en regelgeving vertaald is naar de zorgcontext. De NEN-7510 geeft zicht op de maatregelen die een zorginstelling kan nemen om te voldoen aan de huidige privacywet- en regelgeving. Deze norm is gericht op alle aspecten van informatiebeveiliging. In dit onderzoek ben ik met name geïnteresseerd in de organisatorische kant en de stappen die zorginstellingen in hun communicatie kunnen nemen om te voldoen aan de privacywet- en regelgeving.

Zorginstellingen hebben niet alleen te maken met het beschermen van persoonsgegevens, maar ook met het beschermen van bijzondere persoonsgegevens, waar het gegevens over iemands gezondheid betreft[9]. De hoeveelheid en variatie aan bijzondere persoonsgegevens binnen zorginstellingen maken de beveiliging van deze gegevens en het voorkomen dat de gegevens in de verkeerde handen terecht komen tot een ingewikkelder proces dan in andere sectoren. Ook hebben meer mensen toegang tot de gegevens in de zorgsector dan in

[9] Artikel 16 Wet bescherming persoonsgegevens

andere sectoren. Een patiënt komt op tal van plekken waar zorg verleend wordt, waardoor meer instanties met zijn of haar gegevens te maken hebben. Bovendien zorgt het gebruik van bijzondere persoonsgegevens ervoor dat de lat voor het beschermen van persoonsgegevens voor zorginstellingen hoger ligt dan voor andere sectoren.

Op dit moment besteden zorginstellingen volgens Zandvliet (2016) nog onvoldoende aandacht aan privacy. Ook blijkt uit internationaal onderzoek naar de informatiebeveiliging van 24 ziekenhuizen van Deloitte (2016) dat meer dan de helft van de ziekenhuizen medische apparaten met standaardwachtwoorden heeft en dat bijna de helft van de ziekenhuizen niet onderzoekt of hun medische apparatuur in overeenstemming is met privacywetgeving. Dit betekent dat er bij ziekenhuizen nog veel te winnen is op het gebied van privacy. Oelen (2016) van de Autoriteit Persoonsgegevens geeft aan dat van de meldingen die zij binnenkrijgen 30% afkomstig is uit de gezondheidssector. Er wordt dus wel gemeld in de zorgsector. Hierin hebben zij een vooruitstrevende positie ten opzichte van andere sectoren.

Dit zou verklaard kunnen worden door de meldcultuur die al in zorginstellingen aanwezig is. Naast meldingen voor datalekken bestaan in zorginstellingen namelijk al VIM-meldingen (Veilig Incident Melden). Dit maakt de brug naar het melden van datalekken minder groot. Dankzij de VIM-meldingen en de geheimhoudingsplicht van artsen zijn medewerkers in de zorg al meer bekend met privacygevoelige thema's. Om deze reden mag verwacht worden dat zorginstellingen al bezig zijn met het voldoen aan privacywet- en regelgeving.

2.4 Hoofd- en deelvragen

Om de vraagstelling van dit onderzoek te beantwoorden is het van belang dat de instellingen al bezig zijn met het invullen van de nieuwe privacywet- en regelgeving en hier al stappen in communicatie worden gemaakt. Zoals in paragraaf 2.3 te lezen is, zijn zorginstellingen al bekend met het melden van incidenten en hebben zij een vooruitstrevende positie ten opzichte van andere sectoren. Mede om deze reden is de keuze voor een sector op de zorgsector komen te vallen. Meldingen van datalekken kunnen in de zorgsector binnen de huidige meldsystemen worden ingebouwd, waardoor de stap voor medewerkers minder groot is zich aan te passen aan de nieuwe wet. Zo kan een non-routine matige verandering, meer routinematig worden ingebouwd. Dit maakt het makkelijker om de communicatie in een organisatie vorm te geven. Deze kan van iets uitgebreidere aard zijn dan in een organisatie waarin nog geen kennis is van meldsystemen. Dit maakt de zorgsector tot een geschikte sector om nader in te verdiepen.

In dit onderzoek wordt nagegaan hoe zorginstellingen hun interne communicatie rondom privacybescherming en informatiebeveiliging zo kunnen inrichten dat zij conform de huidige wet- en regelgeving opereren.
Om op deze hoofdvraag een antwoord te formuleren zijn de volgende deelvragen opgesteld:

1. Welke communicatierichtlijnen zijn af te leiden uit bestaande richtlijnen voor zorginstellingen om de interne communicatie rondom privacybescherming en informatiebeveiliging in te richten?

2. Op welke manier wordt in de praktijk invulling gegeven aan de communicatierichtlijnen rondom privacybescherming en informatiebeveiliging?

   Deze vraag is opgesplitst in deelvraag 2a en deelvraag 2b:

   2a Op welke manier wordt door **experts** invulling gegeven aan de communicatierichtlijnen rondom privacybescherming en informatiebeveiliging?

   2b Op welke manier wordt door **zorginstellingen** invulling gegeven aan de communicatierichtlijnen rondom privacybescherming en informatiebeveiliging?

Met deelstudie 1 zal in hoofdstuk 3 antwoord geformuleerd worden op deelvraag 1, waarna met deelstudie 2 in hoofdstuk 4 antwoord geformuleerd zal worden op deelvraag 2. De hoofdvraag zal vervolgens in hoofdstuk 5 beantwoord worden.

3. Studie 1: Documentanalyse

3.1 Vraagstelling van dit onderzoek

In de Wet bescherming persoonsgegevens staat dat een organisatie passende technische en organisatorische maatregelen moet nemen om persoonsgegevens te beveiligen (Autoriteit Persoonsgegevens, 2016). Door deze maatregelen te nemen verkleint een organisatie de kans op datalekken. De zorgsector heeft te maken met bijzondere persoonsgegevens volgens de Wbp. Daarom is het in de zorgsector extra belangrijk om passende technische en organisatorische maatregelen te nemen om persoonsgegevens te beveiligen. In dit hoofdstuk zullen de bestaande richtlijnen voor de zorgsector worden besproken en zullen de communicatierichtlijnen die hiervan af te leiden zijn worden vastgesteld . De centrale vraag hierbij is:

Welke communicatierichtlijnen zijn af te leiden uit bestaande richtlijnen voor zorginstellingen om de interne communicatie rondom privacybescherming en informatiebeveiliging in te richten?

Om te achterhalen wat de Autoriteit Persoonsgegevens onder passende organisatorische maatregelen verstaat, zullen de NEN-7510 norm en de CBP-richtsnoeren gebruikt worden als richtlijn. De NEN-7510 norm is ontwikkeld voor de zorgsector en geeft richtlijnen en uitgangspunten voor het bepalen, instellen en handhaven van maatregelen die een organisatie in de gezondheidszorg moet treffen ter beveiliging van de informatievoorziening (NEN-7510, 2011). De CBP-richtsnoeren zijn ontwikkeld door het CBP om duidelijk te maken wat het CBP van de beveiliging van persoonsgegevens verwacht (CBP-richtsnoeren, 2013). Deze richtsnoeren gelden niet alleen voor de zorgsector, maar ook voor andere sectoren. De algemene richtlijnen uit deze twee instrumenten zijn niet specifiek gericht op de inrichting van de interne communicatie. Daarom zullen in dit hoofdstuk enkel de elementen die betrekking hebben op het inrichten van de interne communicatie besproken worden. Van de organisatorische normen worden enkel die normen gebruikt die voor het goed uitvoeren van het interne communicatiebeleid noodzakelijk zijn.

3.2 Methode

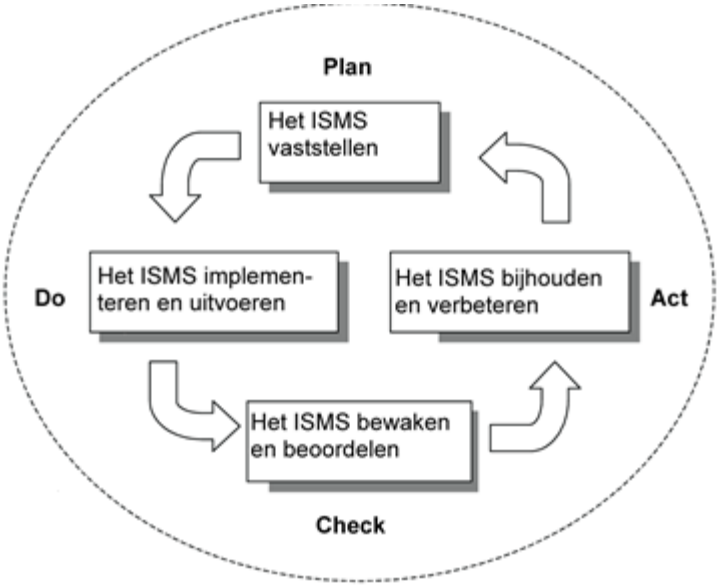
Om zicht te krijgen op de privacywet- en regelgeving die in de zorgpraktijk van belang is, heb ik verschillende landelijke congressen en bijeenkomsten over het thema privacy en dataprotectie bijgewoond. Op deze manier kon ik mij een beeld vormen van het privacythema in de praktijk. Ook heb ik een Ronde Tafel Bijeenkomst van de NGFG met de Autoriteit Persoonsgegevens bijgewoond specifiek over de meldplicht datalekken. Tijdens deze bijeenkomsten werd er over verschillende documenten gesproken zoals de NEN-7510 norm. Dit gaf aanleiding voor mij om mij verder te verdiepen in de bestaande normenkaders. Zo kwam ik er ook achter dat de CBP richtsnoeren had opgesteld. Ik kwam tot de conclusie dat de NEN-7510 norm en de CBP-richtsnoeren een goed uitgangspunt vormden voor het vaststellen van communicatierichtlijnen. Ik heb de documenten uitvoerig bestudeerd en alle richtlijnen van organisatorische aard uit de documenten gefilterd en deze richtlijnen vertaald naar communicatierichtlijnen. In hoofdstuk 3.3 wordt weergegeven hoe deze communicatierichtlijnen zijn afgeleid uit de algemene richtlijnen. De afgeleide communicatierichtlijnen zullen in hoofdstuk 4 gebruikt worden als houvast bij de interviews en er zal gekeken worden hoe er invulling gegeven wordt aan deze richtlijnen door experts en functionarissen gegevensbescherming van zorginstellingen.

3.3 Resultaten

In paragraaf 3.3.1 wordt de plan-do-check-act cyclus geïntroduceerd en daarmee het bredere kader waarbinnen het informatiebeleid wordt vormgegeven, waarna vervolgens per fase van dit model besproken wordt welke rol communicatie hierbij kan spelen.

3.3.1 Richtlijnen naar aanleiding van de wet: Plan-do-check-act cyclus

Het College Bescherming Persoonsgegevens heeft een document met richtsnoeren opgesteld voor de beveiliging van persoonsgegevens. De CBP veronderstelt dat voor een blijvend passend beveiligingsniveau de inbedding van de zogeheten plan-do-check-act cyclus zie Figuur 3 in de dagelijkse praktijk van de organisatie noodzakelijk is.



Plan (het ISMS vaststellen)	Het vaststellen van het ISMS en de doelstellingen, processen en procedures die relevant zijn voor het risicomanagement en verbetering van de informatiebeveiliging, teneinde resultaten te leveren die in overeenstemming zijn met algemene beleidslijnen en doelstellingen van de organisatie.
Do (het ISMS implementeren en uitvoeren)	Het implementeren en uitvoeren van het ISMS, beheersmaatregelen, processen en procedures.
Check (het ISMS controleren en beoordelen)	Beoordelen en, voorzover van toepassing, meten van procesprestaties ten opzichte van het ISMS en de doelstellingen en ervaring uit de praktijk, en rapportage van de resultaten aan de directie ter beoordeling.
Act (het ISMS bijhouden en verbeteren)	Corrigerende en preventieve maatregelen nemen, op basis van de resultaten van de interne ISMS-audit en de directiebeoordeling of andere relevante informatie, om continue verbetering van het ISMS te bewerkstelligen.

Figuur 3: weergave van de plan-do-check-act cyclus (CBP, 2013)

De plan-do-check-act cyclus kan vormgegeven worden in het *Information Security Management System*. Het Information Security Management System (ISMS) is een systematische aanpak om gevoelige bedrijfsinformatie te managen, zodat de bedrijfsinformatie goed beveiligd is. Zowel mensen, processen en IT-systemen maken deel uit van dit systeem. Het systeem maakt gebruik van risicomanagement (ISO27001, 2013). Het baseren van maatregelen op basis van risicomanagement binnen het ISMS zal verder worden toegelicht in paragraaf 3.3.4. In de plan-fase wordt het ISMS vastgesteld, in de do-fase wordt het ISMS geïmplementeerd en uitgevoerd, in de check-fase wordt het ISMS bewaakt en beoordeeld en in de act-fase wordt het ISMS bijgehouden en verbeterd.

3.3.2 Plan-fase: rol van het bestuur

In het vormgeven van het ISMS ligt een belangrijke taak voor het bestuur van de organisatie. De NEN-7510 vereist een actieve betrokkenheid van het bestuur. De directie moet volgens de NEN-7510 bewijs kunnen leveren van haar betrokkenheid met betrekking tot het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van het ISMS. Daarnaast moet de directie in de organisatie het belang kenbaar maken van het voldoen aan doelstellingen voor informatiebeveiliging en het naleven van het informatiebeveiligingsbeleid (NEN-7510, paragraaf 4.2.2).

3.3.3 Plan-fase: randvoorwaarden voor goed beleid

Voordat een organisatie kan beginnen met de plan-fase: het opstellen van privacybeleid, moet de organisatie eerst het bestuur achter zich hebben. In paragraaf 3.3.2 was al te lezen dat de actieve betrokkenheid van het bestuur een vereiste is om te kunnen voldoen aan de NEN-7510. Actieve betrokkenheid van het bestuur draagt ook bij aan de interne communicatie. Als het bestuur zich betrokken opstelt bij het thema dan kan zij dit overdragen naar de rest van de organisatie en ontstaat er een stimulerend klimaat om de privacywet- en regelgeving na te leven[10]. Bovendien helpt een actief betrokken bestuur bij het afstemmen van de interne communicatie op de soort verandering voor medewerkers[11]. Daarom is actieve betrokkenheid van het bestuur een randvoorwaarde voor een goede inrichting van het interne communicatiebeleid.

1. ***Actieve betrokkenheid van het bestuur***
   Een bestuur is volgens de NEN-7510 actief betrokken als het betrokken is bij het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van het beleid. Ook is een bestuur actief betrokken als het belang van privacy duidelijk gemaakt wordt vanuit het bestuur aan de rest van de organisatie. Hiervoor is het een vereiste dat het bestuur zelf het belang van privacy onderkent. Dit kan het bestuur aantonen door bijvoorbeeld privacy op de agenda te zetten van managementoverleggen, een privacyreglement op te stellen voor medewerkers of een budget vrij te maken voor het nemen van maatregelen op het gebied van informatiebeveiliging.

Naast het tonen van actieve betrokkenheid is het ook van belang dat privacy een hoge prioriteit krijgt in de organisatie. Alleen bij een hoge prioriteit voor dit thema zal er namelijk beleid voor worden opgesteld en budget voor worden vrijgemaakt. Bovendien draagt prioriteit voor het thema privacy bij aan het creëren van een stimulerend klimaat. Daarom is de tweede randvoorwaarde voor een goede inrichting van het interne communicatiebeleid:

2. ***Privacy krijgt een hoge prioriteit in de organisatie***
   De risico's van een privacyissue moeten bijvoorbeeld in beeld zijn bij het bestuur en de functie van FG moet duidelijk belegd zijn in de organisatie (NEN-7510, H4). Ook hoort bij deze voorwaarde de taak van het bestuur om het belang van privacy duidelijk te maken aan de rest van de organisatie. Dit gaat verder dan het opstellen van reglementen en het plaatsen op de agenda van privacy. Er zal ook gecommuniceerd moeten worden over het thema privacy naar medewerkers om ervoor te zorgen dat ook zij een hoge prioriteit geven aan privacy.

3.3.4 Plan-fase: randvoorwaarden voor passende maatregelen

Er zijn volgens het CBP twee randvoorwaarden om tot passende maatregelen te kunnen komen: maatregelen op basis van risicoanalyse en het toepassen van beveiligingsstandaarden. In dit onderzoek zal de nadruk liggen op maatregelen op basis van risicoanalyse, omdat de risicoanalyse een rol kan spelen in de manier waarop het communicatiebeleid wordt ingevuld, waar het toepassen van beveiligingsstandaarden meer van technische aard is.

De risicoanalyse bestaat uit het inventariseren van dreigingen die kunnen leiden tot een beveiligingsincident, de gevolgen die dit incident kan hebben en de kans dat deze gevolgen zich voordoen (CBP, 2013). Voordat beleid opgesteld kan worden moet dus eerst een risicoanalyse worden gedaan. Door alle risico's in kaart te brengen kunnen de zwakke plekken in de organisatie gesignaleerd worden en kan hierop ingespeeld worden. Ook in de interne communicatie kan een organisatie hierop inspelen door bijvoorbeeld te kijken waar de grootste risico's liggen bij het lekken van patiëntgegevens door medewerkers en hoe de interne communicatie zo kan worden ingezet dat de grootste risico's worden aangepakt. Dit maakt het doen van een risicoanalyse ook relevant voor de inrichting van de interne communicatie. Communicatierichtlijn 3 is daarom:

3. ***Er is een risicoanalyse gedaan***

[10] Zie paragraaf 2.2.2 model Winkelman (2015) en communicatiedoelstellingen bij een verandering Vos en Schoemaker (2011)

[11] Zie paragraaf 2.2.1 Clampitt (2013) over soort verandering en afstemming hiervan op medewerkers

Vervolgens is het van belang dat de risico's in beeld zijn bij het bestuur, zodat zij op basis van de risicoanalyse beleid op kunnen stellen. Als een organisatie een actief betrokken bestuur heeft, dan mag ervan uitgegaan worden dat het bestuur de risico's van een beveiligingsissue ook in beeld heeft. Toch is het voor een organisatie extra van belang om de risico's van een beveiligingsissue goed in beeld te hebben, aangezien de ingevoerde Wet meldplicht datalekken een grote bestuurlijke verantwoordelijkheid verwacht ten aanzien van dit thema. Mocht er van actieve betrokkenheid van het bestuur nog geen sprake zijn in een organisatie, dan is het tenminste van belang dat de risico's op een beveiligingsissue wel in beeld zijn bij het bestuur. De vierde interne communicatierichtlijn is daarom:

4. De risico's van een beveiligingsissue zijn in beeld bij het bestuur.

3.3.5 Plan-fase: passende maatregelen

Er zijn verschillende soorten maatregelen die een organisatie op basis van risicoanalyse kan nemen:

- *Preventieve maatregelen*
  Voorkomen dat een dreiging leidt tot een beveiligingsincident
- *Detectieve maatregelen*
  Weten dat er een beveiligingsincident heeft plaatsgevonden
- *Repressieve maatregelen*
  Beperken van negatieve gevolgen van het beveiligingsincident
- *Herstelmaatregelen*

Voor interne communicatierichtlijnen zijn vooral preventieve maatregelen van belang. Met behulp van goede interne communicatie kan voorkomen worden dat een dreiging leidt tot een beveiligingsincident.

Bij het onderzoeken en beoordelen van de beveiliging van persoonsgegevens hanteert de CBP als uitgangspunt een aantal beveiligingsmaatregelen die binnen het vakgebied informatiebeveiliging gebruikelijk zijn en die in veel situaties in een of andere vorm noodzakelijk zijn. Hieronder zal ingegaan worden op de maatregelen van organisatorische aard. Hierbinnen richt ik mij met name op de maatregelen die door te voeren zijn in de organisatie zelf met de focus op de rol van de medewerkers en het bestuur binnen de organisatie. Externe partijen zoals samenwerkingen met ketenpartners spelen een minder belangrijke rol voor dit onderzoek.

Als er op bestuurlijk niveau een hoge prioriteit aan privacy wordt gegeven, is de vervolgstap van het bestuur om hier ook naar te handelen en een goed privacybeleid op te stellen. Met behulp van een goed privacybeleid kunnen medewerkers in dit thema worden meegenomen en kunnen ook zij het belang van privacy in gaan zien. De vijfde communicatierichtlijn is daarom:

5. Er is een beleidsdocument 'informatiebeveiliging' aanwezig

Het beleidsdocument gaat expliciet in op de maatregelen die de verantwoordelijke treft om de verwerkte persoonsgegevens te beveiligen. Het document is goedgekeurd op bestuurlijk c.q. leidinggevend niveau en kenbaar gemaakt aan alle werknemers en relevante externe partijen (CBP, 2013; NEN-7510, 2011, paragraaf 5.1.1).

Om te kunnen zien dat informatiebeveiliging prioriteit heeft in de organisatie is het belangrijk dat het beleidsdocument is goedgekeurd op bestuurlijk niveau. Daarnaast moeten medewerkers weten dat het beleidsdocument bestaat.

3.3.6 Do-fase: passende maatregelen

Het opstellen van een beleidsdocument informatiebeveiliging alleen is niet voldoende om medewerkers mee te nemen in dit thema. Er moet ook naar medewerkers gecommuniceerd worden over dit beleid, zoals hierboven wordt aangegeven. De zesde communicatierichtlijn waar organisaties aan moeten voldoen is daarom:

6. Er wordt regelmatig gecommuniceerd over het beleidsdocument informatiebeveiliging

-Medewerkers moeten weten dat het beveiligingsbeleid bestaat[12]
-Medewerkers moeten weten hoe zij het beveiligingsbeleid moeten uitvoeren[13]

Alle werknemers van de organisatie en, voor zover van toepassing, ingehuurd personeel en externe gebruikers krijgen geschikte training en regelmatige bijscholing over het informatiebeveiligingsbeleid en de informatiebeveiligingsprocedures van de organisatie, voor zover relevant voor hun functie. Binnen de training en bijscholing wordt expliciet aandacht besteed aan de omgang met (bijzondere of anderszins gevoelige) persoonsgegevens (CBP, 2013; NEN-7510, paragraaf 8.2.2).

In het theoretisch kader werd al aangegeven dat 80% van de datalekken ontstaat door foutief menselijk handelen. Naast communiceren over het beleid is het daarom van belang bewustzijn te creëren bij medewerkers, zodat zij gaan handelen in lijn met de privacywet- en regelgeving. Het creëren van bewustzijn kan leiden tot een hogere motivatie van medewerkers en een betere bereidheid om volgens de privacywet- en regelgeving te handelen[14]. De zevende communicatierichtlijn is daarom:

7. Er wordt gewerkt aan het verhogen van beveiligingsbewustzijn in de organisatie

Er zijn verschillende mogelijkheden om ervoor te zorgen dat het informatiebeveiligingsbewustzijn in organisaties wordt vergroot. Zo kan bijvoorbeeld een training worden gegeven aan medewerkers. Ook gaat het om de 'regelmatige bijscholing over het beleid en de procedures'. Dit kan op verschillende manieren worden ingevuld. Medewerkers kunnen bijvoorbeeld up-to-date worden gehouden via het intranet, via folders, via nieuwsbrieven en via sociale media.

Om datalekken en beveiligingsincidenten goed af te kunnen handelen is het belangrijk om hiervoor duidelijke procedures op te stellen.

Er zijn procedures voor het tijdig en doeltreffend behandelen van informatiebeveiligingsincidenten en zwakke plekken in de beveiliging, zodra ze zijn gerapporteerd. Het beoordelen van de risico's voor de betrokkenen en het effectief informeren van de betrokkenen en waar van toepassing de toezichthouder is in deze procedures opgenomen. De lessen getrokken uit de afgehandelde incidenten worden gebruikt om de beveiliging waar mogelijk structureel te verbeteren. Als een vervolgprocedure na een informatiebeveiligingsincident juridische maatregelen omvat (civiel of strafrechtelijk) wordt het bewijsmateriaal verzameld, bewaard en gepresenteerd overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd (CBP, 2013; NEN-7510, 2011, paragraaf 13.2).

Er moeten dus duidelijke procedures zijn voor het behandelen van informatiebeveiligingsincidenten en zwakke plekken in de beveiliging. De achtste communicatierichtlijn is daarom:

8. Er zijn duidelijke procedures aanwezig voor het behandelen van informatiebeveiligingsincidenten

Naast dat deze procedures er zijn, is het ook van belang dat deze gecommuniceerd worden naar medewerkers en verspreid worden over de organisatie, zodat iedereen de procedures kent en weet hoe hij/zij volgens deze procedures moet handelen. Ook is de organisatie verantwoordelijk voor het melden van datalekken.

De verantwoordelijke meldt datalekken die onder een wettelijke meldplicht vallen bij de betreffende toezichthouder. Als hij daartoe wettelijk verplicht is of als er anderszins aanleiding voor is informeert hij ook de betrokkenen over het beveiligingsincident of het datalek.

Om de datalekken te kunnen melden aan de toezichthouder moet er een meldcultuur ontstaan in de organisatie. Medewerkers moeten weten waar zij kunnen melden en hoe zij een datalek kunnen herkennen.

De negende communicatierichtlijn is daarom:

[12] Zie paragraaf 2.2.2 Vos en Schoemaker (2011) over de rol van interne communicatie bij veranderingen
[13] Zie paragraaf 2.2.2 Vos en Schoemaker (2011) over de rol van interne communicatie bij veranderingen
[14] Zie paragraaf 2.2.2 Vos en Schoemaker (2011) over communicatiedoelstellingen bij een verandering

9. Er wordt regelmatig over deze procedures gecommuniceerd naar de rest van de organisatie

Er is pas sprake van een passend beveiligingsniveau als de gekozen maatregelen onderdeel zijn van de dagelijkse praktijk van de organisatie. De eerste stap is documentatie: de relevante beveiligingsmaatregelen zijn gespecificeerd en geïntegreerd in functionele en technische beschrijvingen van ICT-systemen, in gebruikershandleidingen, werkinstructies, contracten, dienstenniveauovereenkomsten en andere relevante documenten. De tweede stap is de daadwerkelijke implementatie van de gekozen maatregelen (CBP, 2013).

3.3.7 Check-fase: passende maatregelen

In de check-fase is het van belang om onderdelen van bovenstaande communicatierichtlijnen te evalueren en te kijken of deze richtlijnen worden nageleefd in de organisatie. De tiende communicatierichtlijn is daarom:

10. De gekozen maatregelen worden regelmatig geëvalueerd.

3.3.8 Act-fase: passende maatregelen

In de act-fase is het van belang dat er gehandeld wordt op de informatie die uit de evaluaties naar voren komt en dat het beleid hier eventueel aan wordt aangepast. Communicatierichtlijn nummer elf is daarom:

11. Het beleid wordt na evaluatie indien nodig aangepast.

3.4 Conclusie

In dit hoofdstuk is antwoord gegeven op de vraag:

Welke communicatierichtlijnen zijn af te leiden uit bestaande richtlijnen voor zorginstellingen om de interne communicatie rondom privacybescherming en informatiebeveiliging in te richten?

Uit de analyse van de NEN-7510 en de CBP-richtsnoeren zijn onderstaande elf communicatierichtlijnen voortgekomen.

1. Actieve betrokkenheid van het bestuur
2. Privacy krijgt een hoge prioriteit in de organisatie
3. Er is een risico-inventarisatie gedaan
4. De risico's van een beveiligingsissue zijn in beeld bij het bestuur
5. Er is op basis van de risico-inventarisatie een beleidsdocument informatiebeveiliging opgesteld
6. Er wordt regelmatig gecommuniceerd over het beleidsdocument informatiebeveiliging
7. Er wordt gewerkt aan het verhogen van beveiligingsbewustzijn in de organisatie
8. Er zijn duidelijke procedures aanwezig voor het behandelen van beveiligingsincidenten
9. Er wordt regelmatig over deze procedures gecommuniceerd
10. De gekozen maatregelen worden regelmatig geëvalueerd
11. Het beleid wordt na evaluatie indien nodig aangepast

Deze communicatierichtlijnen vormen het algemene kader waarbinnen het interne communicatiebeleid rondom informatiebeveiliging en privacybescherming van zorginstellingen moet worden vormgegeven. In het volgende hoofdstuk zal met behulp van interviews met experts en functionarissen voor de gegevensbescherming van zorginstellingen gekeken worden hoe en of deze communicatierichtlijnen worden toegepast in de zorgsector.

4. Deelstudie 2: Interviews

4.1 Vraagstelling van dit onderzoek

De geformuleerde communicatierichtlijnen in hoofdstuk 3 bieden houvast bij het kijken naar de invulling van de privacywet- en regelgeving in de zorgsector. De deelvragen die in dit hoofdstuk beantwoord worden zijn:

*2a Op welke manier wordt er door **experts** invulling gegeven aan de communicatierichtlijnen bij het doorvoeren van de nieuwe privacywet- en regelgeving?*

*2b Op welke manier wordt er door **zorginstellingen** invulling gegeven aan de communicatierichtlijnen bij het doorvoeren van de nieuwe privacywet- en regelgeving?*

Er zijn interviews met experts en functionarissen voor de gegevensbescherming van zorginstellingen gehouden om antwoord te formuleren op de twee deelvragen. Deelvraag 2a zal beantwoord worden in hoofdstuk 4.3 en deelvraag 2b zal beantwoord worden in hoofdstuk 4.4. Ten slotte zullen de antwoorden op deelvraag 2a en deelvraag 2b in hoofdstuk 4.5 samengenomen worden tot een antwoord op deelvraag 2:

Op welke manier wordt er invulling gegeven aan de communicatierichtlijnen bij het doorvoeren van de nieuwe privacywet- en regelgeving?

4.2 Methode

De geformuleerde communicatierichtlijnen geven een globaal beeld van de verwachtingen op het gebied van de interne communicatie rondom privacybescherming en informatiebeveiliging. Om een specifieker beeld te krijgen van hoe de interne communicatie rondom privacybescherming en informatiebeveiliging kan worden ingericht zijn interviews afgenomen met experts en met functionarissen gegevensbescherming van zorginstellingen. Er is gekeken hoe er door deze twee groepen op dit moment al invulling gegeven wordt aan de communicatierichtlijnen.

Er is gesproken met vier experts en functionarissen gegevensbescherming van twaalf zorginstellingen. De expertinterviews zijn gebruikt om beter zicht te krijgen op de inhoud van de communicatierichtlijnen en hoe je deze richtlijnen kunt invullen in een organisatie. Onder experts vallen dus mensen van buiten de zorginstellingen, die een bijdrage leveren aan het invullen van de communicatierichtlijnen van zorginstellingen. De experts zijn geselecteerd op hun aanvullende kennis over de onderzoeksthema's.

De interviews met functionarissen gegevensbescherming van zorginstellingen zijn gebruikt om te kijken in hoeverre er in zorginstellingen al invulling gegeven wordt aan de communicatierichtlijnen en op wat voor manier dit gebeurt. Ook geven de interviews met functionarissen gegevensbescherming meer zicht op de mate waarin zorginstellingen al bezig zijn volgens de nieuwe privacywet- en regelgeving te handelen. In 4.2.1 zal eerst besproken worden hoe ik te werk ben gegaan bij de expertinterviews, waarna in 4.2.2 besproken wordt hoe ik te werk ben gegaan bij de interviews met functionarissen voor de gegevensbescherming.

4.2.1 Expertinterviews

Achtergrond experts

De interviews die zijn afgenomen bij experts zijn van semigestructureerde aard. De vastgestelde communicatierichtlijnen zijn als houvast gebruikt. De nadruk lag tijdens de interviews op de communicatierichtlijnen binnen het domein van de expert. Het vaststellen van beleid en het opstellen van procedures is de verantwoordelijkheid van de zorginstelling. Daarom is niet naar de invulling van deze communicatierichtlijnen gevraagd. Deze richtlijnen zijn ook meer voorwaarden voor zorginstellingen om het interne communicatiebeleid vorm te geven en moeten volgens de wet- en regelgeving ingevuld worden. De nadruk lag bij de expertinterviews meer op aanvullende kennis over communicatierichtlijnen die niet op basis van wet- en regelgeving kunnen worden ingevuld, maar waar aanvullende kennis voor nodig is.

Het verhogen van informatiebeveiligingsbewustzijn is bijvoorbeeld één van de communicatierichtlijnen, maar het wordt op basis van deze globale richtlijn niet duidelijk hoe een zorginstelling kan werken aan het verhogen van informatiebeveiligingsbewustzijn. Daarom is aan twee experts met specialisatie in awareness raising programma's gevraagd hun visie te geven op dit vraagstuk. Eén van deze experts heeft daarnaast ook een langdurige opleiding tot FG, waardoor ik meer inzicht kan krijgen in de verschillende facetten die tijdens deze opleiding aan bod komen en in hoeverre interne communicatie op dit moment een rol speelt bij deze opleiding.

Ook krijg ik met behulp van dit interview meer zicht op de functie van de functionaris voor de gegevensbescherming.

Om een breder beeld te krijgen van de manieren waarop de richtlijnen door zorginstellingen kunnen worden ingevuld, zijn ook twee externe privacy officers geïnterviewd. Zij werken voor verschillende zorginstellingen, waardoor zij meer zicht kunnen geven op welke rol interne communicatie speelt binnen zorginstellingen en in welke fase van het doorvoeren van de nieuwe privacywet- en regelgeving deze zorginstellingen zich bevinden. In Tabel 1 staan de achtergronden van de geïnterviewde experts weergegeven.

Tabel 1 Achtergronden geïnterviewde experts

Expert	Functie	Organisatie
Expert 1	Functionaris voor de Gegevensbescherming en initiatiefnemer van het programma Awareness Raising	Duthler Academy
Expert 2	Marketeer en communicatiespecialist en verantwoordelijk voor het opzetten van effectieve security awareness campagnes	Awareways
Expert 3	Manager Business Legal Line	Cure4
Expert 4	Privacy Officer	Cure4

Procedure

Experts zijn via de mail gevraagd om mee te werken aan het onderzoek. Alle gevraagde experts waren bereid mee te werken aan het onderzoek. Er werd een face-to-face afspraak ingepland met de experts op hun werkplek. De interviews duurden zo'n 30-45 minuten. Voor aanvang werd gevraagd of het interview mocht worden opgenomen. Geen van de experts had hiertegen bezwaar. De interviews zijn afgenomen in de periode van 7 tot 30 november 2016.

Analyse

Tijdens de interviews met experts werd dieper ingegaan op hun expertisegebied binnen de communicatierichtlijnen. Daarom was het niet nodig de antwoorden van de experts te categoriseren alvorens ze per richtlijn te bespreken in hoofdstuk 4.3. De uitwerking van het interview werd gebruikt bij het sorteren van de antwoorden per richtlijn. De antwoorden die door experts per richtlijn gegeven zijn, zijn te vinden in hoofdstuk 4.3.

4.2.2 Interviews functionarissen gegevensbescherming

Achtergrond functionarissen gegevensbescherming

Er zijn diepte-interviews gehouden met functionarissen gegevensbescherming van twaalf zorginstellingen. Voorafgaand aan deelname werd informatie gegeven over het onderzoek aan de zorginstellingen. Indien zorginstellingen nog niet bezig waren met het invoeren van beleid rondom informatiebeveiliging en privacybescherming dan konden ze niet deelnemen aan het onderzoek, omdat het van belang was dat er invulling gegeven werd aan de huidige wet- en regelgeving. In totaal zijn er in Nederland 862 zorginstellingen (CBS, 2016) . Deze instellingen variëren enorm in grootte en werk.

Voor dit onderzoek was het van belang een zo breed mogelijk aantal grote zorginstellingen te spreken, van GGZ-instelling tot UMC, omdat de invulling van de nieuwe wet- en regelgeving nog vrij nieuw is en nog geen inschatting gemaakt kan worden hoe de wet wordt ingevuld in de verschillende instanties.

Er is gekozen voor grote zorginstellingen, omdat van deze instellingen verwacht mag worden dat zij meer budget en mogelijkheden hebben om de nieuwe privacywet- en regelgeving door te voeren. Ook hebben zij te maken met grotere hoeveelheden patiëntgegevens en veel medewerkers, waardoor het risico op een datalek met imagoschade als gevolg groter is in deze instellingen. Dit kan ertoe leiden dat grote instellingen

eerder stappen zullen nemen om invulling te geven aan de nieuwe privacywet- en regelgeving. Hun invulling aan de wet- en regelgeving kan als voorbeeld dienen voor andere zorginstellingen, die deze stappen ook zullen moeten nemen.

Er zijn in totaal 32 zorginstellingen benaderd. Hiervan gaven vier zorginstellingen aan niet mee te willen werken aan het onderzoek. Van tien zorginstellingen is geen reactie of een te late reactie op het verzoek gekomen en zes zorginstellingen gaven aan nog niet ver genoeg te zijn om te kunnen deelnemen aan dit onderzoek. Tabel 2 geeft een overzicht van de samenstelling van de zorginstellingen.

Tabel 2 Samenstelling zorginstellingen

Geïnterviewde	Soort zorginstelling
A	UMC
B	Ziekenhuis
C	Thuiszorg
D	GGZ
E	GGZ
F	Ziekenhuis
G	GGZ
H	UMC
I	Thuiszorg
J	Ziekenhuis
K	UMC
L	GGZ

Procedure

Tijdens het benaderen van de zorginstellingen ontdekte ik dat de zorginstellingen alleen mee wilden werken als informatie niet tot hun instelling herleidbaar was. Daarom heb ik hierop geanticipeerd door met een privacyverklaring (bijlage 1) te garanderen dat de informatie niet herleidbaar zou zijn naar de instelling. De zorginstellingen werden via een LinkedInoproep en via de mail gevraagd of zij mee wilden werken aan het onderzoek. De gegevens van functionarissen gegevensbescherming van zorginstellingen werden via het register van de Autoriteit Persoonsgegevens en via mijn contacten achterhaald. In de mail werd uitleg gegeven over het onderzoek.

Met de zorginstellingen die reageerden dat ze mee wilden werken, werd een face-to-face afspraak ingepland. De interviews duurden 45-60 minuten. Vooraf werd toestemming gevraagd aan de geïnterviewde om het gesprek op te nemen. De geïnterviewden hadden hier geen van allen bezwaar tegen. Na een korte kennismaking en introductie van het onderzoek werd gestart met het interview. De interviews zijn afgenomen in de periode 31 oktober t/m 6 december 2016 en vonden plaats in de betreffende zorginstelling.

De interviews waren semigestructureerd van aard. Er is gebruik gemaakt van een vooraf opgestelde topiclijst om ervoor te zorgen dat de communicatierichtlijnen die in het vorige hoofdstuk besproken zijn ook in de interviews naar voren kwamen. Tijdens het interview werden een aantal hoofdthema's besproken in wisselende volgorde:

- De functie van Functionaris voor de Gegevensbescherming
- De belegging van de functie in de organisatie
- Informatiebeveiligingsbeleid
- Communicatie over informatiebeveiligingsbeleid
- Gevolgen van datalek
- Betrokkenheid van bestuur
- Prioriteit van privacy in de organisatie
- Meldplicht datalekken
- Communicatie over meldplicht datalekken

In bijlage 2 staat de topiclijst die gebruikt is als houvast tijdens de interviews. Hierin staan naast de hoofdthema's ook de onderwerpen waarover gesproken is binnen deze hoofdthema's. Het thema 'de functie van functionaris voor de gegevensbescherming' diende vooral om meer zicht te krijgen op waar deze functie uit bestaat in de verschillende organisaties en vanuit welke achtergronden de functie wordt in gevuld. Het thema 'de belegging van de functie in de organisatie' diende vooral om meer zicht te krijgen op hoe de functionaris voor de

gegevensbescherming in verband stond met de rest van de organisatie (heeft hij/zij bijvoorbeeld een strategische positie met inbreng in het bestuur?).

Met behulp van de thema's 'informatiebeveiligingsbeleid' en 'communicatie over informatiebeveiligingsbeleid' kon achterhaald worden of er een informatiebeveiligingsbeleid was en in hoeverre er communicatie over dit beleid was in de organisatie. Gevraagd werd bijvoorbeeld naar de inzet van communicatiemiddelen en de bekendheid met bestaande campagnes. Het thema 'gevolgen van een datalek' gaf zicht op of een organisatie de risico's van een beveiligingsissue kan herkennen en of er op basis van risicoanalyse beleid wordt opgesteld.

Binnen de thema's 'betrokkenheid van het bestuur' en 'prioriteit van privacy in de organisatie' ging het vooral om de aandacht die er vanuit het bestuur aan dit thema wordt gegeven. De thema's 'meldplicht datalekken' en 'communicatie over meldplicht datalekken' gaven zicht op de veranderingen in de organisatie sinds de invoering van de Wet meldplicht datalekken en of er in de organisatie procedures aanwezig zijn om volgens deze wet te handelen. Ook is gevraagd naar de communicatie over deze meldplicht.

Het hanteren van een topiclijst had als voordeel dat er ruimte was voor mij om door te vragen binnen de communicatierichtlijnen aan de hand van de gegeven antwoorden van de respondenten. Aangezien de communicatierichtlijnen vrij algemeen waren hielp dit mij beter begrip te krijgen van hoe de interne communicatie van een zorginstelling wordt ingericht en wat hier allemaal bij komt kijken.

Analyse

Er is gekozen voor een letterlijke weergave van de interviews om de objectiviteit van het onderzoek en de betrouwbaarheid te vergroten. Eén geïnterviewde ging niet akkoord met deze manier van weergeven. Daarom is van deze zorginstelling enkel een zakelijke samenvatting te vinden in bijlage 5.6. De topiclijst is gebruikt als houvast bij het categorisatieproces. De complete uitwerking van het interview werd onderverdeeld in thema's. Thema's die niet op de topiclijst stonden zijn extra toegevoegd. Alle interviews werden eerst op deze manier uitgewerkt, waarna gekeken werd waar verbanden zaten tussen de besproken thema's. Op deze manier kon het aantal besproken thema's teruggebracht worden en konden de thema's ondergebracht worden onder een aantal hoofdthema's. Dit leidde uiteindelijk tot de verdeling zoals deze is weergegeven in het codeboek in bijlage 3.

De gecategoriseerde versies van de interviews zijn vervolgens gebruikt om te kijken hoe de richtlijnen zijn ingevuld in de zorginstellingen. Per richtlijn is gekeken wat de geïnterviewde van de zorginstelling hierover zegt. De gecategoriseerde versies gaven overzicht van de besproken thema's wat dit proces vergemakkelijkte. Thema's waarin niks over communicatierichtlijnen stond zijn niet meegenomen in de losse analyse per interview die te vinden is in bijlage 7 en de samenvatting van de analyse per interview in bijlage 8. In de resultatensectie hieronder zal per communicatierichtlijn besproken worden hoe deze werd ingevuld door de zorginstellingen.

4.3. Resultaten expertinterviews

De uitwerkingen van de interviews met experts zijn te vinden in bijlage 3. In dit hoofdstuk worden de belangrijkste resultaten besproken. De experts helpen allen de organisaties bij het werken met de nieuwe privacywet- en regelgeving. In hoofdstuk 3 zijn elf communicatierichtlijnen geformuleerd voor zorginstellingen. De experts helpen organisaties bij het invullen van deze richtlijnen. In paragraaf 4.3.1 wordt besproken hoe de richtlijnen worden ingevuld door experts. De communicatierichtlijnen zijn in eerste instantie opgesteld voor zorginstellingen, waardoor niet alle richtlijnen voor experts relevant zijn. Het opstellen van een informatiebeveiligingsbeleid en het opstellen van procedures zijn bijvoorbeeld onderdeel van het beleid van zorginstellingen. Experts spelen hierin een minder belangrijke rol. In paragraaf 4.3.2 zal het belang van de FG-functie als extra onderwerp besproken worden.

4.3.1 Invulling van communicatierichtlijnen door experts

Actieve betrokkenheid van het bestuur

Expert 2 geeft onder andere managementsessies om het belang van privacy onder de aandacht te brengen op bestuurlijk niveau en het bestuur bij het onderwerp te betrekken. Ook zorgt expert 2 er aan het begin van een traject voor dat zij met verschillende groepen om tafel zit, waaronder ook het bestuur. Expert 2: 'Wij vragen dan vaak of we om tafel kunnen met IT, communicatie, HR en iemand van de board, omdat dit belangrijke mensen zijn om te betrekken in dit verhaal'.

Expert 3 geeft aan dat het belangrijk is om aansluiting te zoeken bij de organisatie, bijvoorbeeld bij iemand van het bestuur. Het teamwork binnen de organisatie is namelijk ook van belang. 'Dit is bijvoorbeeld van belang voor de adviezen die wij geven en de protocollen die wij uitwerken. Deze moeten geborgd worden in de

organisatie, naast dat ze geïmplementeerd moeten worden. Als we dat in ons eentje opstellen, zonder back-up vanuit de organisatie, dan krijg je het niet voor elkaar'. Expert 3 haalt daarom het liefst iemand van het bestuur erbij. Er moet ook altijd gerapporteerd worden aan het bestuur, dus die back-up is enorm belangrijk.

Expert 2 geeft aan dat beveiliging de verantwoordelijkheid is van de hele organisatie en niet alleen van IT. Je moet op zoek gaan naar de overkoepelende doelstelling en vragen wat ieders verantwoordelijkheid daarin is. Op termijn is het dus van belang dat niet alleen het bestuur actief betrokken is, maar ook andere afdelingen. Expert 2 geeft aan: 'Wij zijn er om begrip te krijgen tussen de afdelingen en aan te geven dat je zonder optimale beveiliging niet verder kan'.

Prioriteit van privacy in de organisatie

Om de prioriteit van privacy te vergroten in organisaties ontwikkelt expert 2 onder andere trendsessies waarbij op board en c-level organisaties geïnspireerd worden door hen te laten zien waar we over tien jaar staan en wat dat betekent voor hun medewerkers, voor security awareness en voor technische beveiliging. Volgens expert 2 helpt dit organisaties om verder te kijken dan alleen nu brandjes te blussen. Op deze manier krijgt privacy een hogere prioriteit in de organisatie. Ook doet expert 2 aan red teaming: 'Dan kijken we hoe makkelijk we ergens binnenkomen en confronteren we daar vervolgens de board mee'. De prioriteit voor privacy wordt ook vergroot door het geven van ambassadeursessies en managementsessies. Expert 2 probeert er daarnaast voor te zorgen dat informatiebeveiliging en informatiebewustzijn een topic blijft binnen de organisatie door nauw samen te werken met communicatie en HR. 'We proberen vaak met organisaties om het ook binnen de HR-cyclus te krijgen zodat het ook echt onderdeel wordt van het functioneren van iemand'.

Expert 3 geeft aan dat op het moment dat ze een training gegeven hebben de prioriteit meteen hoger wordt. 'Dan komen er ineens heel veel dingen naar boven in de organisatie. Medewerkers worden meer betrokken, omdat ze ook beter geïnformeerd zijn. Ze stellen bijvoorbeeld zelf meer kritische vragen zoals: "ik heb nu hiermee te maken is dit misschien een datalek?" Of: "Mag ik dit wel of niet mailen?" En dat krijgen we inderdaad ook terug vanuit de bestuurders. Medewerkers worden ineens wakker en dan zie je de prioriteit ook stijgen'.

Het doen van een risico-inventarisatie

Expert 2 doet een risico-inventarisatie op het gebied van awareness door de mate van volwassenheid binnen een organisatie te meten. Dit doet expert 2 op basis van zes variabelen van gedrag. Daarvoor gebruikt expert 2 de Theory of Planned Behaviour uit de psychologie. 'We meten de norm binnen de organisatie, we meten wat de houding is en een houding die kun je weer onderverdelen in: is het beschikbaar, is het relevant en is er interesse. Dan meten we het kenniscomponent. We meten de controle die mensen ervaren en het uiteindelijke gedrag. En op al die facetten scoren we een organisatie en dan zien we waar een organisatie slecht op scoort'. Expert 2 geeft aan dat het veel voorkomt dat organisaties slecht scoren op de norm. Het is bijvoorbeeld niet de cultuur van een organisatie om een computer te locken of iemand erop aan te spreken als die het niet goed doet.

Expert 2 ziet ook problemen in kennis. Mensen weten bijvoorbeeld niet hoe ze phishingmails moeten herkennen of mensen weten niet wanneer een wachtwoord veilig is. Ook expert 4 houdt voorafgaand aan het geven van een training een enquête, zodat het altijd een training op maat is voor de organisatie. Er wordt geïnventariseerd wat de status van een organisatie is, zodat gekeken kan worden wat voor training nodig is.

Expert 3 geeft aan dat organisaties soms ook zelf een privacy QuickScan willen om te weten waar ze staan. Met de QuickScan toetsen expert 3 en 4 bijvoorbeeld hoe bewust medewerkers al zijn. Expert 3 geeft aan dat je eigenlijk ook de vervolgstap moet doen: een Privacy Impact Assessment. 'De QuickScan is een eerste stap. Wij noemen het ook wel nulmeting. Expert 4 geeft aan dat PIA's veel completere en uitgebreidere analyse geven. De verschillende diensten van de zorginstelling worden dan getoetst. Expert 3 geeft bovendien aan dat het wel belangrijk is om bij de klant aanwezig te zijn om te zien wat er op de werkvloer gebeurt. Expert 4 sluit hierbij aan en geeft aan dat je dan ook meer feeling krijgt bij de organisatie en meer inzicht in alle processen bij de klant.

Risico's in beeld bij organisatie

Expert 1 gebruikt het awareness raising programma om risico's in beeld te brengen bij de organisatie. In een e-learningmodule wordt steeds één onderwerp besproken. Er wordt besproken wat de risico's zijn en hoe deze vermeden kunnen worden. Expert 2 maakt gebruik van een scenario waarin verschillende situaties van een willekeurige werkdag uit het leven van een actrice te zien zijn. Dit laat zien in welke situaties je op een dag terecht komt waar mogelijke risico's zich voordoen. 'Van ik stap in de trein, naar ik ben op mijn werk, naar ik heb een afspraak buiten de deur, naar ik ga weer terug naar huis. Wat kom je dan tegen? Expert 2 brengt risico's ook

onder de aandacht met behulp van red teaming. Expert 4 geeft aan dat zowel boetes als imagoschade een heikel punt zijn voor organisaties.

Communiceren over informatiebeveiligingsbeleid
Expert 2 kijkt samen met de communicatieafdeling hoe het onderwerp kan worden ingebouwd in de jaarlijkse interne communicatiekalender. Expert 3 geeft aan dat medewerkers moeten weten bij wie ze moeten melden, hoe ze moeten melden en dat ze eventueel aanvullende informatie kunnen aangeven. Expert 3 en 4 maken soms gebruik van communicatiemiddelen, zoals het ophangen van een quote of het geven van uitleg over bepaalde thema's via de mail, maar zijn nog niet actief bezig met communiceren over het informatiebeveiligingsbeleid.

Het werken aan het verhogen van het beveiligingsbewustzijn
Tijdens het volgen van de opleiding tot FG ontdekte expert 1 dat privacy meer een organisatievraagstuk is dan een juridisch vraagstuk. Daarom is ze een programma Awareness Raising gestart. Dit programma helpt organisaties bij het verhogen van het beveiligingsbewustzijn van hun medewerkers. Onderdeel van dit programma is het volgen van een e-learning. Expert 1 geeft hierover aan: 'Iedereen in de organisatie moet dit volgen, niet alleen ICT-mensen, maar dit is voor iedereen van belang'.

Dit Programma Awareness Raising kent drie niveaus, omdat niet iedereen in de organisatie met dezelfde onderwerpen te maken heeft. Op het basisniveau leer je wat privacy is, waar het vandaan komt en wat de wetgeving is. Dit niveau is voor iedereen in de organisatie. Op het tweede niveau ga je dieper in op privacy en doen mensen mee die wel veel doen met persoonsgegevens, maar niet veel werken met bijzondere persoonsgegevens en geen leidinggevend personeel. Het derde niveau is voor leidinggevenden en mensen die werken met bijzondere persoonsgegevens. De onderwerpen die in de e-learningmodules besproken worden zijn: introductie en doel, beveiliging, persoonsgegevens, werkplek en omgeving, datalek en veilig internetgebruik. Het programma wordt gekenmerkt door herhaling en het is een langdurig programma.

Ook expert 2 is gestart met een programma Awareness Raising. Expert 2 maakt hierbij gebruik van een breed pakket aan e-learningmodules die het informatiebeveiligingsbewustzijn van medewerkers verhogen. Daarnaast geeft expert 2 ook managementsessies en ambassadeurssessies om mensen verantwoordelijk te maken in de organisatie. Deze mensen worden verantwoordelijk voor privacy en informatiebeveiliging binnen hun afdeling, waardoor een organisatie steeds meer vertegenwoordigers van het thema krijgt en het thema dus meer aandacht krijgt binnen de organisatie. 'Ook doen we wel eens eerst een ambassadeurssessie voordat we beginnen met de e-learning. Tijdens zo'n sessie proberen we te inspireren, interesseren en shockeren. Dan heb je mensen al geprimed en dan zijn mensen positiever voor ze zo'n e-learning gaan doen, omdat we hun houding al beïnvloed hebben'. Expert 2 organiseert bovendien personeelsbijeenkomsten waar ook criticasters aanwezig zijn. Zij zijn kritisch en hebben daar een reden voor. Expert 2 gaat dan op zoek naar hun weerstanden.

Met de e-learningmodules probeert expert 2 mensen zelf te laten nadenken over het thema om op deze manier het beveiligingsbewustzijn te vergroten. 'Wij leren mensen nadenken. Je moet als medewerker het risicoprofiel van bepaalde activiteiten inschatten. Dat gaat over met wat voor informatie werk ik? Waar werk ik? Hoe ga ik het verwerken? En mag ik het verwerken? Dus elke keer als jij met een activiteit bezig bent moet je dat in je hoofd afspelen.'

Expert 2 geeft aan: 'Awareness is een doorlopend onderwerp en daarom proberen we het ook binnen communicatie op de agenda te krijgen als onderwerp. Uiteindelijk is een organisatie zelf verantwoordelijk om de beveiliging op niveau te houden en daar hoort awareness ook bij, dus kun je ervoor kiezen om sessies te blijven herhalen'. Expert 4 geeft aan dat het werken aan het verhogen van beveiligingsbewustzijn met name met trainingen gebeurt: 'Ja we hangen wel eens quotes op of uitleg over bepaalde onderwerpen en we sturen informatie rond, maar we gebruiken met name trainingen. De mensen krijgen we met de trainingen over het algemeen wel mee'. Door het gebruiken van de antwoorden van medewerkers op de vragen uit de enquête wordt de training levendig gehouden, omdat medewerkers hun eigen praktijkvoorbeelden in de training kunnen herkennen.

Expert 1, 2, 3 en 4 werken dus allemaal aan het verhogen van beveiligingsbewustzijn in organisaties met behulp van e-learning of training. Ter aanvulling op de e-learning worden door expert 2 management- en ambassadeursessies gegeven om de motivatie van medewerkers om de e-learning te gaan volgen te vergroten. Het programma Awareness Raising van expert 1 zit nog in de opstartfase, waardoor het pakket dat deze expert aanbiedt nog wat minder uitgebreid is, maar in de toekomst wil expert 1 dit pakket zeker uitbreiden naar managementsessies en het aanbieden van diensten aan bijvoorbeeld de communicatieafdeling.

Evaluatie van prestaties organisaties
Expert 1 geeft aan dat om een module van de e-learning af te ronden de medewerker een test moet doen. De uitkomsten van deze test zijn bepalend of je door mag naar de volgende module. Expert 2 evalueert continu de campagnes die ze doet: 'Zeker, want awareness valt ook onder de KPI's inmiddels en de meting daar kunnen we heel veel cijfers uit halen en ook de e-learning is allemaal meetbaar'.

4.3.2 Het belang van een goede functionaris gegevensbescherming

De persoon die als eerste in aanraking komt met het toezien op de privacywet- en regelgeving is de functionaris voor de gegevensbescherming in de organisatie. Vanaf mei 2018, wanneer de Europese Verordening handhaafbaar wordt, is het verplicht om een functionaris voor de gegevensbescherming aan te stellen voor organisaties die op grote schaal persoonsgegevens verwerken (AVG, 2016). Veel organisaties hebben daarom een functionaris gegevensbescherming aangesteld. Dit zijn vaak mensen met een juridische of ICT-achtergrond (Expert 1). Zij komen bijvoorbeeld vanuit een andere functie in de organisatie in de functie van FG, maar hebben hier geen speciale opleiding voor gevolgd.

Toch moet een FG van een boel zaken verstand hebben. Expert 1 is daarom begonnen aan een opleiding tot FG bij Duthler Academy. Dit is een tweejarige opleiding met dertig modules waarin alle aspecten van de functie FG behandeld worden. 'De modules worden continu aangepast en vernieuwd aan de veranderende wetgeving, want er veranderen ook altijd dingen in de praktijk' zo stelt expert 1. Je kunt bij Duthler Academy kiezen voor een volledige opleiding of voor een aantal modules. Daarnaast heb je stepup cursussen voor managers en bestuursraden, zodat zij in een paar dagen bijgepraat raken op dit thema. Expert 1 merkt in de praktijk dat juristen vaak veel ervaring hebben met privacywetgeving, maar niet met de nieuwe wetgeving en dat dit wel belangrijk is. Ook ziet ze tot haar spijt dat functionarissen voor de gegevensbescherming op dit moment onvoldoende kennis hebben om hun functie goed te vervullen. Zeker omdat een FG in een organisatie een beschermde titel heeft, is het van belang dat hier iemand zit met verstand van zaken.

4.3.3 Deelconclusie 1

Met behulp van de antwoorden van experts kan een antwoord geformuleerd worden op deelvraag 2a:

2a Op welke manier wordt er door experts invulling gegeven aan de communicatierichtlijnen voor het doorvoeren van de nieuwe privacywet- en regelgeving?

De experts geven aan dat actieve betrokkenheid van het bestuur van belang is. Adviezen moeten namelijk geborgd worden in de organisatie en het bestuur is eindverantwoordelijk voor het melden van datalekken. Een organisatie kan actieve betrokkenheid bijvoorbeeld realiseren door managementsessies te houden en door begrip te creëren tussen afdelingen.

Experts geven verschillende manieren aan waarop prioriteit voor privacy in een organisatie gerealiseerd kan worden. Een organisatie kan bijvoorbeeld managementsessies, trendsessies of ambassadeurssessies organiseren. Ook kan gedacht worden aan het geven van een training en het onderdeel maken van privacy van het functioneringsgesprek. Om het belang van privacy ook op bestuurlijk niveau onder de aandacht te brengen kan van buitenaf ook gedacht worden aan red teaming (hoe gemakkelijk komt een buitenstaander binnen in de organisatie).

Experts doen een risico-inventarisatie voor de betreffende organisatie alvorens zij hun werkzaamheden gaan verrichten. Dit kan een privacy QuickScan, een privacy volwassenheidsscore of een Privacy Impact Assessment betreffen.

Om risico's in beeld te brengen bij de organisatie is red teaming een manier. Ook is het een idee om de risico's te bespreken in een e-learningmodule.

Communiceren over het informatiebeveiligingsbeleid gebeurt door de experts waarmee gesproken is niet uitgebreid, omdat hun focus hier niet op ligt. Dit is meer iets voor intern in de organisatie. Wel helpen experts de organisatie soms op weg door bijvoorbeeld met de communicatieafdeling te kijken hoe het onderwerp kan worden ingebouwd in de interne communicatiekalender of door af en toe iets op te hangen of uit te leggen over bepaalde thema's.

Experts helpen organisaties bij het verhogen van beveiligingsbewustzijn door het geven van e-learnings of trainingen. Om de motivatie bij medewerkers te vergroten om de e-learning te doen kan een management- of ambassadeurssessie helpen.

Op het gebied van evaluatie van de prestaties van organisaties worden bijvoorbeeld tests gedaan aan het einde van e-learningmodules. De e-learnings zijn meetbaar, waardoor er veel cijfers en informatie uitgehaald kunnen worden.

Naast bovenstaande richtlijnen, gaf één expert aan dat het ook van belang is een goed opgeleide FG te hebben, omdat de functie van FG een beschermde titel is en een FG van veel verschillende thema's verstand moet hebben, zoals juridische, ICT en organisatorische thema's. Het hebben van een goed opgeleide FG kan dus toegevoegd worden aan de communicatierichtlijnen.

Het overzicht van communicatierichtlijnen uit hoofdstuk 3 kan dankzij de interviews met experts worden aangevuld en de invulling van de richtlijnen door experts kan worden toegevoegd aan dit overzicht. Het aangepaste overzicht is weergegeven in Tabel 3 en vormt tevens het antwoord op deelvraag 2a. Hierin zijn sommige communicatierichtlijnen iets anders geformuleerd dan in hoofdstuk 3 om ze van toepassing te maken op experts in plaats van zorginstellingen.

Tabel 3 Invulling van communicatierichtlijnen door experts

Communicatierichtlijn	Invulling van richtlijn experts
Actieve betrokkenheid van het bestuur	• Managementsessies organiseren • Begrip proberen te creëren tussen afdelingen
Prioriteit voor privacy in de organisatie	• Managementsessies, trendsessies of ambassadeurssessies organiseren • Training geven • Onderdeel maken van functioneren medewerker • Red teaming
Inventariseren van risico's	• Uitvoeren van Privacy QuickScan • Uitvoeren van Privacy Impact Assessment • Volwassenheidsniveau van bewustwording meten
Risico's in beeld bij organisatie	• Risico's bespreken in e-learningmodule • Red teaming
Opstellen van informatiebeveiligingsbeleid	Het is de verantwoordelijkheid van de organisatie dat dit beleid er is. De invulling hiervan kan per organisatie verschillen. Experts zijn daarom niet bevraagd over dit thema.
Communiceren over het informatiebeveiligingsbeleid	Ook met deze richtlijn houden de geïnterviewde experts zich niet primair bezig. Wel helpen experts organisaties soms op weg door bijvoorbeeld met de communicatieafdeling te kijken hoe het onderwerp kan worden ingebouwd in de interne communicatiekalender of door iets op te hangen of uit te leggen in de organisatie.
Werken aan beveiligingsbewustzijn	• E-learning • Trainingen • Managementsessies • Ambassadeurssessies
Opstellen van procedures	Het is de verantwoordelijkheid van de organisatie dat deze procedures er zijn. De invulling hiervan kan per organisatie verschillen. Experts zijn daarom niet bevraagd over dit thema.
Communiceren over procedures	Dit is eveneens de verantwoordelijkheid van de organisatie. Experts zijn niet bevraagd naar dit thema.
Evalueren van prestaties van organisaties	• Meetbaar maken van e-learning • Tests laten doen door medewerkers
Aanschaffen van een goed opgeleide functionaris voor de gegevensbescherming	Voorwaarde voor goed uitvoeren beleid.

4.3 Resultaten interviews zorginstellingen

Hieronder zullen de resultaten van de interviews met functionarissen gegevensbescherming van zorginstellingen besproken worden. De uitwerking en categorisatie van de interviews zijn te vinden in bijlage 5 en 6. In dit hoofdstuk zal per communicatierichtlijn besproken worden wat de belangrijkste resultaten waren. De losse analyses per instelling en de samenvatting van deze analyses zijn te vinden in bijlage 7 en 8.

4.3.1 Actieve betrokkenheid van het bestuur

De indeling van zorginstellingen van een wel actief betrokken en niet actief betrokken bestuur staat weergegeven in Tabel 4. Hieronder zal worden toegelicht wanneer een bestuur als actief betrokken wordt beschouwd en wanneer niet.

Tabel 4 Zorginstellingen ingedeeld op betrokkenheid van het bestuur

Betrokkenheid	Zorginstelling
Actief betrokken	B, C, D, E, G, H, J, L
Wel betrokken, maar niet actief	A, K, F
Niet betrokken	I

Acht van de twaalf zorginstellingen hebben een actief betrokken bestuur (B, C, D, E, G, H, J, L). De zorginstellingen verschillen in de mate waarin het bestuur betrokken is. Als het bestuur actief deelneemt aan overleggen en evaluaties dan weegt dit zwaarder dan wanneer het bestuur meer een passieve rol aanneemt zoals het goedkeuren van beleid.

Er zijn bijvoorbeeld drie (A, K en F) zorginstellingen waar documenten over het informatiebeveiligingsbeleid wel langs de Raad van Bestuur gaan, maar waar de Raad van Bestuur geen actieve rol speelt in het vormgeven van het informatiebeveiligingsbeleid. Een voorbeeld hiervan is zorginstelling A (UMC). A geeft aan dat de vragen en ideeën binnen het thema privacy meestal vanuit de privacycommissie geregeld worden. De brieven die de organisatie stuurt en de rapportages datalekken gaan wel langs de Raad van Bestuur. Er is ook een bestuurslid dat privacy in zijn portefeuille heeft. Het bestuur wordt in zorginstelling A dus wel betrokken bij het beleid, maar speelt geen actieve rol in het vormgeven van beleid.

Bij zorginstelling B wordt het bestuur actief betrokken bij het privacybeleid. Over de actieve betrokkenheid bij het melden van datalekken zegt B dat het bestuur hoofdelijk aansprakelijk is op het moment dat het fout gaat dus hij vindt het heel logisch dat zij degene zijn die daar een eindoordeel over vellen. Ook heeft B met beide leden van het bestuur maandelijks contact. Bij één zorginstelling is helemaal geen sprake van betrokkenheid van het bestuur (I).

In Tabel 5 staat weergegeven welke kenmerken van een actief betrokken bestuur genoemd werden en wordt aangegeven in welke interviews over dit kenmerk gesproken werd. In Tabel 6 wordt aangegeven welke kenmerken genoemd werden van een niet betrokken bestuur.

Tabel 5 Kenmerken van een actief betrokken bestuur

Kenmerk	Genoemd in interview
Het bestuur staat achter het beleid	B, E, F, G, H, J
Het bestuur is verantwoordelijk voor de meldingen	B, C, G, H, L
Rapportages gaan langs het bestuur	A, H, J, L
Een bestuurslid is portefeuillehouder van privacy	A, H, J, L
Incidenten worden besproken met bestuur	B, C, L
Leden van bestuursstaf zitten in privacyteam	C, E
Er is maandelijks contact met bestuur	B, D
Brieven gaan langs bestuur	A
Privacy is vast onderwerp op agenda van managementoverleggen	H

Tabel 6 Kenmerken van een niet betrokken bestuur

Kenmerk	Genoemd in interview
Vragen en ideeën over privacy worden vanuit de privacycommissie geregeld, het bestuur komt hier niet bij kijken	A, K
Er gebeurt niks met voorgesteld beleid	L
Meldingen naar AP worden gedaan door privacyteam	K

4.3.2 Prioriteit van privacy in de organisatie

De indeling van zorginstellingen naar wel of geen prioriteit voor privacy staat weergegeven in Tabel 7. Hieronder zullen een aantal voorbeelden genoemd worden uit de interviews die aangeven hoe deze indeling naar prioriteit tot stand komt aan de hand van de antwoorden van functionarissen gegevensbescherming.

Tabel 7 Zorginstellingen ingedeeld op prioriteit

Prioriteit	Zorginstelling
Wel	A, C, D, E, F, G, J, K
Geen of lage	B, I, L

Van de twaalf zorginstellingen geven er negen (A, C, D, E, F, G, H, J, K) aan dat privacy in hun organisatie prioriteit heeft. De mate van prioriteit verschilt nogal tussen de negen zorginstellingen. Bij zorginstelling H (UMC) zien we dat privacy een hoge prioriteit heeft. Zorginstelling H beschikt over een afdeling privacybescherming en informatiebeveiliging. In dit team zitten vier personen. Hierin zitten drie FG's en één documentalist. Ook aan de onderzoekkant van het UMC is gedacht en hier is een aparte FG voor aangesteld. Een incident in het verleden heeft er mede voor gezorgd dat privacy nu hoog op de prioriteitenlijst staat bij zorginstelling H. Het staat als vast onderwerp op de agenda en één van de leden van de Raad van Bestuur heeft privacy in zijn portefeuille.

A geeft een aantal argumenten waarom privacy wel prioriteit heeft, maar daarnaast ook argumenten waarom privacy geen prioriteit heeft. A geeft aan dat de Raad van Bestuur natuurlijk wel heeft ingestemd met het oprichten van de privacywerkgroep, het aanstellen van A als extra functionaris voor de gegevensbescherming en dat één bestuurslid privacy in zijn portefeuille heeft en het ook wel belangrijk vindt. Tegelijkertijd geeft A aan dat de andere bestuursleden daar iets minder feeling mee hebben en dat je bij dit onderwerp te maken hebt met verschillende mensen: 'De één vindt het heel belangrijk, de ander vindt het irritante onzin'.

Er zijn drie zorginstellingen waar privacy geen of een lage prioriteit heeft (B, I, L). Zorginstelling I is één van deze instellingen. Bij zorginstelling I liggen van allerlei documenten ter goedkeuring bij de Raad van Bestuur, maar daar gebeurt niks mee. Ook geeft I aan dat privacy en security gewoon niet op de agenda staat. I: 'Ja, dat hebben we allemaal wel, we hebben ook gewoon een leerportaal en trainingen en dat soort zaken. Het is allemaal wel beschikbaar, maar privacy en security staat gewoon niet op de agenda'.

Een overzicht van de kenmerken die in de interviews genoemd zijn van prioriteit voor privacy zijn te zien in Tabel 8. Een overzicht van de kenmerken die genoemd zijn van geen prioriteit zijn te vinden in Tabel 9.

Tabel 8 Kenmerken van prioriteit van privacy

Kenmerk	Genoemd in interview
Er is een privacywerkgroep	A, C, E, H, J
Er is een (extra) FG aangesteld	A, E, H
Privacy staat op de agenda van managementoverleggen en/of teamoverleggen	C, H, J
Top straalt uit dat privacy belangrijk is	G, H, K
Privacy staat in top 5/risicoprofiel van Raad van Bestuur	H, K, J
Er is een bestuurslid dat privacy in zijn portefeuille heeft	A
Privacy is een terugkerend thema	F
Raad van bestuur is bereid om budget uit te geven	J

Tabel 9 Kenmerken geen prioriteit voor privacy

Kenmerk	Genoemd in interview
Raad van Bestuur geeft niet aan dat er aandacht moet worden gegeven aan privacy	B
Er is geen budget voor privacythema's	B
Hoger management maakt fouten in basisregels en geeft dus geen goed voorbeeld	D
Er gebeurt niks met voorgesteld beleid	L
Teammanagers vinden het maar onzin	J
Privacy staat niet op de agenda	L

4.3.3 Er is een risico-inventarisatie gedaan

In alle instellingen is een risico-inventarisatie of nulmeting gedaan om te kijken waar de zorginstelling staat op het gebied van privacybescherming en informatiebeveiliging. De NEN-7510 wordt vaak als uitgangspunt genomen, waaraan de instelling moet gaan voldoen. Genoemde risico's zijn bijvoorbeeld de risico's bij een datalek zoals reputatieschade, de boete en het verlies van patiëntvertrouwen.

Zorginstelling L geeft aan dat de risico's van een datalek voor hen vooral aan de zachte kant zitten: 'Informatiebeveiliging heeft twee kanten, een harde kant en een zachte kant. En de harde kant hebben wij vrij goed ingericht denk ik. We hebben een deel van onze IT ook geoutsourcet en daar ook allerlei afspraken gemaakt met de leverancier. Maar wat je ziet is je kunt je netwerk, je applicaties, wel goed beveiligen, maar als mensen zich daar niet aan houden bijvoorbeeld aan wachtwoorden, aan autorisaties, dan kom je ook niet ver'.

Ook worden door een aantal instellingen technische risico's genoemd. Zorginstelling K geeft bijvoorbeeld aan dat de belangrijkste verstoringen stroomstoringen, storingen in de infrastructuur en dat de patiënten niet meer in het ziekenhuis kunnen komen zijn.

4.3.4 De risico's van een beveiligingsissue zijn in beeld bij het bestuur

Eén geïnterviewde van de zorginstellingen wist niet of de risico's in beeld waren bij het bestuur. A: 'Ik sta dan toch iets te ver af van de Raad van Bestuur om te weten hoe zij ernaar kijken, dat weet ik eigenlijk niet zo goed'. De overige elf instellingen hebben wel aangegeven of de risico's in beeld zijn bij het bestuur. De mate waarin de risico's in beeld zijn van het bestuur verschilt nogal per zorginstelling.

In drie zorginstellingen (B, E, G) worden bijvoorbeeld de boetes meteen als risico genoemd. B geeft aan dat er heel veel aandacht is voor de boetes die je kunt krijgen. En G zegt: 'Nou ja goed zijn deze gevolgen in beeld bij het bestuur, ja dat ligt eraan of je een boete gaat krijgen of niet'.

Zes zorginstellingen zien naast de boetes ook nog andere risico's (C, D, F, H, J, L). Door zorginstelling H wordt reputatieschade als meest beducht genoemd en zorginstelling F geeft aan wat de gevolgen zijn van een datalek: 'Los van die boete heb je als organisatie ook een klus die je moet uitvoeren als je met een datalek van doen hebt. Je moet ontdekken wat de oorzaak van het lek is, wat de gevolgen van het lek zijn en wat je daaraan kunt doen. Daarnaast heb je herstelwerkzaamheden als ziekenhuis om aan het basisprincipe te kunnen voldoen dat iedere patiënt op je moet kunnen vertrouwen'. Het verlies van patiëntvertrouwen wordt dus ook als belangrijk risico gezien. In twee zorginstellingen lijken de risico's niet in beeld te zijn bij het bestuur (I en K).

4.3.5 Er is een beleidsdocument informatiebeveiliging opgesteld

In alle twaalf instellingen is een beleidsdocument informatiebeveiliging opgesteld of vergelijkbare documenten zoals privacybeleid, privacyreglementen en gedragscodes. Zorginstelling A heeft daarnaast ook een checklist informatiebeveiliging. Dit is een checklist voor personeel om te kijken of ze voldoende rekening houden met informatiebeveiliging.

4.3.6 Er wordt regelmatig gecommuniceerd over het beleidsdocument informatiebeveiliging

In Tabel 10 staat weergegeven in welke zorginstellingen regelmatig gecommuniceerd wordt over het beleidsdocument informatiebeveiliging en in welke zorginstellingen dit niet het geval is.

Tabel 10 Zorginstellingen ingedeeld op regelmatige communicatie over beleidsdocument

Regelmatige communicatie	Zorginstelling
Wel	A, B, C, F, G, H, J
Niet	D, E, I, K, L

Er zijn grote onderlinge verschillen in de mate waarin in zorginstellingen over informatiebeveiliging gecommuniceerd wordt. In vijf zorginstellingen wordt niet regelmatig gecommuniceerd over informatiebeveiliging (D, E, I, K en L). Zorginstelling D geeft aan: 'Op dit moment wordt er niet heel veel anders gedaan dan gecommuniceerd via het digitale documentatiesysteem. Het meer push zoals posters en nieuwsberichten moet nog komen'. In de overige zeven zorginstellingen wordt wel regelmatig gecommuniceerd over informatiebeveiliging.

Zorginstelling F heeft een breed communicatiepakket. F geeft voorlichting en adviseert gevraagd en ongevraagd. Daarbij beweegt F zich door de hele organisatie, dus vanaf de werkvloer tot aan de Raad van Bestuur. Ook houdt F een presentatie voor nieuwe medewerkers en gaat F bij afdelingen langs om presentaties te geven over informatiebeveiliging, privacy en de meldplicht datalekken. Zorginstelling F is al zes jaar aan de slag met communiceren rondom informatiebeveiliging en het is dan ook een terugkerend thema.

Zorginstelling A, B, C, G, H en J maken ook gebruik van verschillende communicatiemiddelen, maar zijn niet zo actief bezig met communiceren over informatiebeveiliging als zorginstelling F. Zorginstelling A organiseert bijvoorbeeld jaarlijks de dag van de patiëntveiligheid in de vorm van een markt en houdt jaarlijks bijeenkomsten en zorginstelling J geeft medewerkers brochures bij indiensttreding en de serviceassistenten van zorginstelling J hadden een training informatiebeveiliging. J2 doet daarnaast veel werkoverleggen en geeft voorlichting. Bij zorginstelling J is echter geen goede samenwerking met de afdeling communicatie. J1 en J2 proberen voornamelijk zelf het wiel uit te vinden.

4.3.7 Er wordt gewerkt aan het verhogen van beveiligingsbewustzijn in de organisatie

In Tabel 11 staat weergegeven in welke zorginstellingen gewerkt wordt aan het verhogen van beveiligingsbewustzijn en in welke organisaties niet.

Tabel 11 Zorginstellingen ingedeeld op werken aan verhogen beveiligingsbewustzijn

Werken aan beveiligingsbewustzijn	Zorginstelling
Wel	A, C, F, G, H, J, L
Niet	B, D, E, I, K

In zeven zorginstellingen wordt gewerkt aan het verhogen van beveiligingsbewustzijn (A, C, F, G, H, J, L). In sommige hiervan wordt actiever gewerkt aan het verhogen van beveiligingsbewustzijn dan in andere. Zo heeft zorginstelling L een e-learning en zijn ze aan het kijken naar de mogelijkheden voor een bewustwordingscampagne.

In zorginstelling H wordt op verschillende manieren gewerkt aan het verhogen van beveiligingsbewustzijn. H1: ‘We hebben sowieso van die posters, do’s en don’ts, we doen gebouwrondes. Iedere twee maanden doen we zo’n gebouwdeel en dan leggen we een soort kaarten neer met smileys met achterop wat wel en wat niet kan. We merken dat dat een heel sterk awarenessbevorderend effect heeft, want als we ergens een ronde gedaan hebben, worden we meteen heel vaak gebeld’. Ook is zorginstelling H bezig met het ontwikkelen van e-learningmodules, heeft zorginstelling H twee sites voor informatiebeveiliging en privacybescherming en krijgen nieuwe medewerkers bij binnenkomst een praatje.

In vijf zorginstellingen (B, D, E, I, K) wordt (nog) niet gewerkt aan het verhogen van beveiligingsbewustzijn. Bij zorginstelling I en E zijn er al wel plannen voor het werken aan beveiligingsbewustzijn, maar deze zorginstellingen bevinden zich nog in de beginfase van het doorvoeren van het beleid en zijn er dus nog niet mee bezig om het beveiligingsbewustzijn te vergroten.

4.3.8 Er zijn duidelijke procedures aanwezig voor het behandelen van beveiligingsincidenten

In elf van de twaalf zorginstellingen zijn al procedures aanwezig voor het behandelen van beveiligingsincidenten. Van drie van deze zorginstellingen zijn deze procedures vrij globaal beschreven (C, D en G). Zorginstelling C heeft bijvoorbeeld een interne meldingsprocedure voor datalekken, maar deze wordt nog niet zo vaak gebruikt. Ook heeft zorginstelling C geen algemeen calamiteitenplan. Zorginstelling D geeft aan dat je op twee manieren kunt melden bij je leidinggevende of via het incident-meldsysteem. Er is op dit moment echter alleen nog een privacydocument aanwezig waarin staat dat je een datalek moet melden en waar, maar er is geen campagne of apart schemaatje om alles te versimpelen. Eén zorginstelling heeft nog geen actieve procedures voor het behandelen van beveiligingsincidenten (I).

De overige acht instellingen hebben een duidelijkere procedure voor datalekken. In het datalekprotocol van zorginstelling E staan verschillende mogelijkheden om te melden: je kunt melden via e-mail, je leidinggevende informeren of een veiligheidsmelding doen. Het privacyteam gaat vervolgens aan de slag en stelt eventueel vragen aan de lijnorganisatie. Na een melding wordt afhankelijk van de aard van de melding teruggekoppeld aan de medewerker.

Zorginstelling H is nog specifieker over hun procedure datalekken. Naast het bellen, mailen en meldsysteem is het bijvoorbeeld ook mogelijk dat er meldingen binnenkomen via de beveiliging bijvoorbeeld van een gestolen laptop, via de sociale media of via de helpdesk ICT.

Ook wordt door H1 uitvoerig beschreven hoe een datalek behandeld wordt: 'Dan doen wij de eerste beoordeling en indien het een ernstig incident is dan nemen wij meteen contact op met de secretaris van de Raad van Bestuur dan vindt er een beoordeling plaats en dan wordt gekeken of we dat in een kleine setting kunnen afhandelen. Dat betekent wij toetsen aan de wet en kijken of we melding moeten doen aan de AP en of betrokkenen geïnformeerd moeten worden en dergelijke en op die manier geven we een advies en dat neemt de Raad van Bestuur dan over of niet en wij zorgen dat het uitgevoerd wordt, maar bij een ernstig incident wordt het hele circus opgetrommeld. Iemand uit de Raad van Bestuur wordt de voorzitter van de beheersgroep. Daar zit ook de directeur communicatie en daar zit de voorzitter van de commissie privacybescherming in en daar zitten wij in en daar zit de directeur ICT bij en de technical security officer die kennis heeft van de harde informatiebeveiliging dus heel technisch. En dan komen we afhankelijk van de ernst: één of meerdere keren per dag bij elkaar zal ik maar zeggen. En dan wordt daar netjes verslag van gemaakt en we bouwen een dossier op. De procedure is eigenlijk heel kort en krachtig. Het zijn eigenlijk maar drie velletjes en dat is ook eigenlijk de kracht van de procedure iedereen weet meteen wat hij moet doen en wij zijn eigenlijk degenen die dan het proces sturen'.

4.3.9 Er wordt regelmatig over deze procedures gecommuniceerd

In Tabel 12 staat weergegeven welke zorginstellingen regelmatig over de procedures communiceren en welke niet.

Tabel 12 Zorginstellingen ingedeeld op regelmatige communicatie over de procedures

Regelmatige communicatie procedures	Zorginstelling
Wel	A, B, C, E, F, G, J, K
Niet	D, I, L*

**Informatie over zorginstelling H ontbreekt, omdat er in dit interview niet specifiek gesproken is over het communiceren van procedures.*

Bij één zorginstelling is niet specifiek gesproken over het communiceren over de procedures (H). Van de overige elf zorginstellingen communiceren er acht regelmatig over de procedures (A, B, C, E, F, G, J, K). Een voorbeeld hiervan is zorginstelling K. Zorginstelling K communiceert op veel verschillende manieren over de procedures. K heeft wat teksten gemaakt voor de Raad van Bestuur en is de eerste helft van het jaar de organisatie ingegaan met presentaties in de afdelingen bij MT's van de divisies om te vertellen wat informatiebeveiliging is en wat privacy betekent en wat je moet doen als iets niet goed gaat.

Een aantal divisies hebben dit zelf opgepakt. K: 'We hebben het eerste half jaar geventileerd van jongens we willen graag wat vertellen over dit onderwerp. We hebben het MT benaderd, de Manager Bedrijfsvoering die dit in zijn portefeuille heeft en gezegd: 'u kunt zelf een presentatie geven of wij komen toelichting geven in een teamoverleg'. K geeft aan dat de divisies waar ze langs zijn geweest nu ook erg actief bezig zijn met informatiebeveiliging. Bij zorginstelling K mogen divisies zelf keuzes maken in de manier van communiceren. K: 'Er zijn bijvoorbeeld divisies die zeggen van doe voor ons een presentatie of een stukje tekst, maar we hebben een website waar we intern op kunnen publiceren, we hebben nieuwsbrieven die we kunnen publiceren'.

Ook heeft K in samenwerking met een marketingadviseur een geplastificeerd a4tje met een aantal spelregels erop met wat doe je wel en wat doe je niet door het huis verspreid en op de website geplaatst.

De drie andere zorginstellingen communiceren niet regelmatig over de procedures (D, I, L). Bij zorginstelling L is er bijvoorbeeld nog geen specifiek communicatiebeleid voor communiceren over de procedures en bij zorginstelling I is er nog geen sprake van lopende procedures, dus wordt hier ook niet over gecommuniceerd.

4.3.10 Het gekozen beleid wordt regelmatig geëvalueerd en indien nodig aangepast

Deze twee richtlijnen zijn in de bespreking samengenomen, omdat het vaak over dezelfde aanpassing gaat bij het aanpassen en evalueren van beleid. De zorginstellingen waren in de meeste gevallen nog niet ver genoeg om over regelmatige evaluatie van het informatiebeveiligingsbeleid te spreken. B zou bijvoorbeeld wel graag willen dat er casussen worden besproken op de afdelingen, maar dat is op dit moment nog niet het geval.

Ook D zou dit graag willen: 'Nee, als er een groot onderzoek is geweest omdat er een calamiteit is geweest. Dat komt niet op intranet van dit zijn de bevindingen geweest en dit zijn de verbetermaatregelen en hé jongens wil iedereen daar even op letten, terwijl dat in mijn ogen wel goed zou zijn om dat wel te doen. Je moet natuurlijk altijd oppassen dat je niet ook de privacy van de medewerkers schendt, maar ja met een beetje goede wil'.

Er werden door een aantal zorginstellingen wel voorbeelden voor evalueren van beleid genoemd. Er gaan bijvoorbeeld wel rapportages datalekken naar de Raad van Bestuur bij zorginstelling A en L en zorginstelling C geeft aan dat als iets vaker voorkomt ze dat wel meenemen. Ook issues waarvan C denkt dat ze daar wat mee moeten in de organisatie koppelt C terug aan de stuurgroep en dan geeft C daar advies over. Dan bepaalt de bestuurder of hij het advies wel of niet overneemt, dus dat komt wel iedere keer terug in de cyclus.

In zorginstelling C is ook geconstateerd dat er geen meldingen worden gedaan (ook geen MIC en MIM meldingen). Er is door deze instelling gekeken hoe dit anders kan en toen is het beleid aangepast. Het verandert echter nog steeds niet.

Bij zorginstelling E worden incidenten gezien als leermomenten. E: 'Dus we gebruiken het om alerter te worden en om te ontdekken waar bijvoorbeeld zwakke plekken zitten in onze infrastructuur en dat kan leiden tot een advies van 'joh we moeten het anders gaan doen'. Een voorbeeld van zo'n incident is dat er zeventien meldingen binnenkwamen dat er cliëntendossiers bij de printer bleven liggen. E: 'We hebben natuurlijk getoetst van hoe kan dat nou dat dat gebeurt want we hebben toch de mogelijkheid om beveiligd te printen. Maar ze kunnen kiezen om dat niet te doen en dan is de vraag van 'goh hoe breng je dat nu onder de aandacht van 1800 medewerkers?' Het advies van E was om een proefconcept te starten met follow-me printen. Mensen hebben dan maar één printer en kunnen niet meer kiezen.

In zorginstelling D is beleid ook na evaluatie aangepast. Eerst had zorginstelling D allemaal losse versies van SPSS maar die stonden op laptops die mensen meenamen en dat vond zorginstelling D wel een risico. Dat heeft zorginstelling D verbeterd door een netwerkversie aan te schaffen. Nu hoeven onderzoekers niks extern meer te doen, want ze kunnen thuis ook inloggen op het systeem.
In zorginstelling F wordt aangegeven dat de evaluatie van communicatie nog wel wat beter zou kunnen. F heeft wel een actielijst voor dingen die aangepast moeten worden om te gaan voldoen aan de AVG in 2018.

Bij zorginstelling H worden incidenten geëvalueerd en worden er interne en externe audits gedaan.
Bij zorginstelling J en K worden incidenten ook geëvalueerd. J2 geeft aan dat je ook bij werkoverleggen hoort waar medewerkers tegenaan lopen. Ook controleert J2 op afdelingen of ze iets doen aan informatiebeveiliging.

4.3.11 Deelconclusie 2

Met behulp van bovenstaande resultaten kan antwoord gegeven worden op deelvraag 2b:

2b Op welke manier wordt er door zorginstellingen invulling gegeven aan de communicatierichtlijnen voor het doorvoeren van de nieuwe privacywet- en regelgeving?

Er wordt op diverse manieren invulling gegeven aan de geformuleerde communicatierichtlijnen door zorginstellingen. Sommige zorginstellingen zijn hier wat verder mee dan andere en gebruiken verschillende manieren om de communicatierichtlijnen in te vullen. In Tabel 14 wordt een overzicht gegeven van de manier van invulling van de communicatierichtlijnen door zorginstellingen. Uit de interviews met de zorginstellingen

bleek dat wanneer zorginstellingen spraken over evaluatie zij ook spraken over hoe het beleid als gevolg hiervan aangepast werd. Daarom zijn deze twee communicatierichtlijnen samengenomen tot één.

Tijdens het onderzoek bleek dat de geïnterviewde grotere ziekenhuizen en UMC's een minder betrokken bestuur hebben dan de kleinere ziekenhuizen en GGZ-instellingen. Toch scoren deze instellingen niet minder op het invullen van de overige communicatierichtlijnen, de UMC's scoren hier zelfs hoger op. Het kan dus zijn dat in deze instellingen een 'normaal' betrokken bestuur al voldoende is en het bestuur niet per se actief betrokken hoeft te zijn bij de uitvoering van het privacybeleid. Dit kan ook te maken hebben met de organisatiecultuur die heerst in deze instellingen. In grotere ziekenhuizen en UMC's wordt gewerkt met verschillende divisies, waardoor veel verantwoordelijkheid in deze divisies ligt.

Het onderzoek is uitgevoerd onder zorginstellingen die al dusdanig bezig waren met privacybescherming en informatiebeveiliging dat ze antwoord konden geven op vragen hierover. Dit betekent dat er ook genoeg zorginstellingen zijn die zich nog niet in dit stadium bevinden. Deze zorginstellingen zullen eerst moeten zorgen voor een duidelijk beleid en een duidelijke verdeling van verantwoordelijkheden alvorens zij zich bezig kunnen houden met communicatierichtlijnen.

Bij sommige communicatierichtlijnen ging het om de voorwaarde dat iets aanwezig was in een instelling. Als er bijvoorbeeld geen informatiebeveiligingsbeleid is dan kan er ook geen communicatie over plaatsvinden. In deze gevallen staat achter de communicatierichtlijn enkel aangegeven hoeveel van de zorginstelling aan deze richtlijn voldaan hebben.

Tabel 13 Invulling van communicatierichtlijnen door zorginstellingen

Communicatierichtlijn	Invulling van richtlijn zorginstellingen
Actieve betrokkenheid van het bestuur	• Het bestuur staat achter het beleid • Het bestuur is verantwoordelijk voor meldingen • Rapportages gaan langs het bestuur • Een bestuurslid is portefeuillehouder van privacy • Incidenten worden besproken met bestuur • Leden van bestuursstaf zitten in privacyteam • Er is maandelijks contact met bestuur • Brieven gaan langs bestuur • Privacy is een vast onderwerp op de agenda van managementoverleggen
Prioriteit voor privacy in de organisatie	• Er is een privacywerkgroep • Er is een (extra) FG aangesteld • Privacy staat op de agenda van managementoverleggen en/of teamoverleggen • Top straalt uit dat privacy belangrijk is • Privacy staat in top 5 /risicoprofiel van Raad van Bestuur • Er is een bestuurslid dat privacy in zijn portefeuille heeft • Privacy is een terugkerend thema • Raad van Bestuur is bereid om budget uit te geven

(Tabel vervolgt op de volgende pagina)

Communicatierichtlijn	Invulling van richtlijn zorginstellingen
(Vervolg van tabel op vorige pagina)	
Risico's in beeld bij organisatie	Bij zes van de twaalf zorginstellingen zijn de risico's goed in beeld bij het bestuur
Opstellen van informatiebeveiligingsbeleid	In alle geïnterviewde zorginstellingen is een informatiebeveiligingsbeleid opgesteld
Communiceren over het informatiebeveiligingsbeleid	Zeven zorginstellingen communiceren regelmatig over het beleidsdocument informatiebeveiliging. Voorbeelden van communicatie zijn: • Het geven van voorlichting en adviezen • Het houden van presentaties op alle afdelingen • Het houden van presentaties aan nieuwe medewerkers • Een evenement organiseren • Het maken van een brochure • Het geven van een training informatiebeveiliging • Het onder de aandacht brengen op werkoverleggen
Werken aan beveiligingsbewustzijn	In zeven van de twaalf zorginstellingen wordt gewerkt aan het verhogen van beveiligingsbewustzijn. Manieren om te werken aan beveiligingsbewustzijn: • E-learning • Posters • Do's en don'ts • Gebouwrondes • Bewustwordingscampagne • Website • Praatje voor nieuwe medewerkers
Opstellen van procedures	In elf van de twaalf zorginstellingen zijn procedures aanwezig voor het behandelen van beveiligingsincidenten.
Communiceren over procedures	Door acht van de elf* zorginstellingen wordt regelmatig gecommuniceerd over de procedures. Manieren waarop dit gedaan wordt door zorginstellingen: • Presentaties op afdelingen • Website • Nieuwsbrieven • A4tje met spelregels
Evalueren en aanpassen van beleid	In de meeste gevallen waren zorginstellingen nog niet ver genoeg om over regelmatige evaluatie van het informatiebeveiligingsbeleid te spreken.

**Informatie over zorginstelling H ontbreekt, omdat er in dit interview niet specifiek gesproken is over het communiceren van procedures.*

4.4 Conclusie

In deze gezamenlijke conclusie van hoofdstuk 4.2 en 4.3 zal antwoord geformuleerd worden op deelvraag 2:

Op welke manier wordt er invulling gegeven aan de communicatierichtlijnen voor het doorvoeren van de nieuwe privacywet- en regelgeving?

Uit de interviews met experts en functionarissen gegevensbescherming blijkt dat er op tal van manieren invulling gegeven wordt aan de opgestelde communicatierichtlijnen. Een overzicht van de invulling van de communicatierichtlijnen is te zien in Tabel 15. De inzichten die zijn voortgekomen uit de interviews met experts en die toepasbaar zijn op zorginstellingen zijn in dit overzicht verwerkt. Deze tabel geeft tevens antwoord op deelvraag 2.

Twee richtlijnen zijn meer voorwaarden om de interne communicatie goed te kunnen inrichten dan dat er verschillende manieren bestaan om invulling te geven aan deze richtlijnen. Het betreft hier de richtlijnen: opstellen van informatiebeleid en opstellen van procedures. Het evalueren en aanpassen van beleid is bovendien organisatieafhankelijk, dus over deze richtlijn kunnen geen algemene instructies voor het invullen ervan gegeven worden. Ook hier kan alleen afgevinkt worden of het wel of niet gebeurt in zorginstellingen.

Verder lijkt het een idee om de communicatierichtlijn: ‘risico’s zijn in beeld bij het bestuur’ onder te verdelen onder actieve betrokkenheid van het bestuur, aangezien dit aantoont dat een bestuur betrokken is bij het onderwerp. Er kwamen ook niet veel inzichten uit de antwoorden op deze vraag vanuit zorginstellingen, er werd enkel aangegeven of het bestuur wel of geen risico’s in beeld heeft. Dus het lijkt een logische keuze om deze communicatierichtlijn te laten vervallen en onder te brengen bij ‘actieve betrokkenheid van het bestuur’. Experts gaven wel enkele manieren om de risico’s in beeld te brengen bij het bestuur, maar dit waren externe manieren en deze manieren waren meer gericht op het onder de aandacht brengen van risico’s bij de gehele organisatie dan enkel bij het bestuur.

De invulling van communicatierichtlijnen door experts verschilt in sommige opzichten van die van zorginstellingen. Zo houden experts zich uitgebreider bezig met één thema, zoals het verhogen van beveiligingsbewustzijn, waar functionarissen gegevensbescherming van zorginstellingen zich met alle communicatierichtlijnen moeten bezighouden. Door de diepgang van de experts zijn uitgebreidere methoden duidelijk geworden om aandacht te besteden aan het verhogen van beveiligingsbewustzijn dan bij zorginstellingen duidelijk werd. Ook is meer ingetreden op details bij experts, zoals hoe een e-learning eruit kwam te zien en uit welke onderdelen deze bestaat.

Experts zijn bovendien buitenstaanders, terwijl functionarissen voor de gegevensbescherming van zorginstellingen zich veelal in de organisatie bevinden. Hierdoor konden experts van een afstand zicht geven op zaken als hoe realiseer je actieve betrokkenheid en hoe zorg je voor een hoge prioriteit van privacy, terwijl de functionarissen voor de gegevensbescherming een indruk gaven van of er op dit moment sprake was van actieve betrokkenheid en hoge prioriteit in hun organisatie en wat de kenmerken hiervan waren.

Tabel 14 Overzicht van de manieren waarop zorginstellingen invulling kunnen geven aan de communicatierichtlijnen

Communicatierichtlijn	Hoe?
Actieve betrokkenheid van het bestuur	• Het bestuur staat achter het beleid • Het bestuur is verantwoordelijk voor meldingen • Rapportages gaan langs het bestuur • Een bestuurslid is portefeuillehouder van privacy • Incidenten worden besproken met bestuur • Leden van bestuursstaf zitten in privacyteam • Er is maandelijks contact met bestuur • Brieven gaan langs bestuur • Privacy is een vast onderwerp op de agenda van managementoverleggen • Begrip creëren tussen afdelingen • Risico's in beeld bij het bestuur
Prioriteit voor privacy in de organisatie	• Er is een privacywerkgroep • Er is een goed opgeleide (extra) FG aangesteld • Privacy staat op de agenda van managementoverleggen en/of teamoverleggen • Top straalt uit dat privacy belangrijk is • Privacy staat in top 5 /risicoprofiel van Raad van Bestuur • Er is een bestuurslid dat privacy in zijn portefeuille heeft • Privacy is een terugkerend thema • Raad van Bestuur is bereid om budget uit te geven • Onderdeel maken van functioneren medewerker
Inventariseren van risico's	• Uitvoeren van Privacy QuickScan • Uitvoeren van Privacy Impact Assessment • Volwassenheidsniveau van bewustwording meten
Opstellen van informatiebeveiligingsbeleid	Voorwaarde

(Tabel vervolgt op volgende pagina)

Communicatierichtlijn	Hoe?
(Vervolg van tabel op vorige pagina)	
Communiceren over het informatiebeveiligingsbeleid	• Het geven van voorlichting en adviezen • Het houden van presentaties op alle afdelingen • Het houden van presentaties aan nieuwe medewerkers • Een evenement organiseren • Het maken van een brochure • Het geven van een training informatiebeveiliging • Het onder de aandacht brengen op werkoverleggen
Werken aan beveiligingsbewustzijn	• E-learning • Posters • Do's en don'ts • Gebouwrondes • Bewustwordingscampagne • Website • Praatje voor nieuwe medewerkers • Managementsessies • Ambassadeurssessies
Opstellen van procedures	Voorwaarde
Communiceren over procedures	• Presentaties op afdelingen • Website • Nieuwsbrieven • A4tje met spelregels
Evalueren en aanpassen van beleid	Organisatieafhankelijk hoe dit wordt ingevuld

5. Conclusie

In dit onderzoek is gekeken naar de inrichting van de interne communicatie van zorginstellingen om te kunnen opereren conform de nieuwe privacywet- en regelgeving. De hoofdvraag hierbij was:

Hoe kunnen zorginstellingen hun interne communicatie rondom privacybescherming en informatiebeveiliging zo inrichten dat zij conform de huidige wet- en regelgeving opereren?

In hoofdstuk 3 zijn communicatierichtlijnen vastgesteld voor zorginstellingen om hun interne communicatie rondom privacybescherming en informatiebeveiliging in te richten. De geïnterviewde experts en zorginstellingen bleken al bezig te zijn met het invullen van deze communicatierichtlijnen, waardoor er verschillende methodes om invulling te geven aan deze communicatierichtlijnen naar voren kwamen in de interviews. Met behulp van de interviews werd bovendien inzichtelijk dat sommige communicatierichtlijnen meer een voorwaarde waren om aan andere communicatierichtlijnen te kunnen voldoen. Ook werd duidelijk dat het hebben van een goed opgeleide functionaris voor de gegevensbescherming van belang is voor de inrichting van het beleid. De inzichten uit de interviews en documentanalyse kunnen vertaald worden naar adviezen voor de zorgsector om hun interne communicatie rondom privacybescherming en informatiebeveiliging in te richten. Deze adviezen luiden als volgt:

1. Zorg voor actieve betrokkenheid van het bestuur

Een zorginstelling kan actieve betrokkenheid realiseren door een bestuurslid portefeuillehouder van privacy te maken of door leden van de bestuursstaf onderdeel te maken van het privacyteam. Andere mogelijkheden zijn om het bestuur verantwoordelijk te maken voor meldingen om op deze manier incidenten bespreekbaar te maken op bestuursniveau en risico's van beveiligingsincidenten scherp in beeld te houden.

2. Zorg voor prioriteit van privacy

Om volgens de huidige privacywet- en regelgeving te kunnen opereren moet een zorginstelling aan kunnen tonen dat privacy hoge prioriteit heeft. Dit kan een zorginstelling bijvoorbeeld doen door een privacywerkgroep of een goed opgeleide (extra) functionaris voor de gegevensbescherming aan te stellen, door privacy op de agenda te zetten van vergaderingen, door budget vrij te maken voor privacy of door het onderdeel te maken van het functioneren van de medewerker.

3. Breng risico's van beveiligingsissue's in kaart en stel op basis daarvan een informatiebeveiligingsbeleid op

Een zorginstelling kan risico's in kaart brengen door een Privacy Impact Assessment te doen of privacynulmeting afhankelijk van het stadium waarin de instelling zich bevindt. Een Privacy Impact Assessment is uitgebreider dan een nulmeting, waardoor een instelling aan meer eisen moet voldoen. Op basis van deze risicoanalyse kan een zorginstelling vervolgens een informatiebeveiligingsbeleid opstellen, waarbij de hoogste prioriteit uitgaat naar de hoogste risico's en hoe deze worden aangepakt. Belangrijk bij dit punt is dat er niet alleen gelet wordt op de risico's op een boete of op risico's van technische aard, maar dat ook organisatorische risico's worden meegenomen, zoals mogelijke reputatieschade en het verlies van patiëntvertrouwen.

4. Communiceer over het informatiebeveiligingsbeleid en werk aan het verhogen van beveiligingsbewustzijn

Een zorginstelling kan gebruik maken van verschillende communicatiemiddelen om te communiceren over het informatiebeveiligingsbeleid. Zo kan een zorginstelling voorlichting geven, presentaties houden of een brochure maken, waarin uitleg gegeven wordt over het informatiebeveiligingsbeleid. Op deze manier kan kennis over het informatiebeveiligingsbeleid en de bijbehorende regels gemakkelijk verspreid worden over de organisatie. Voor het verhogen van beveiligingsbewustzijn moet een zorginstelling nog een stapje verder gaan. Hiervoor is namelijk ook de motivatie van medewerkers nodig om volgens de nieuwe wet- en regelgeving te handelen. Dit betekent dat het simpelweg presenteren van het beleid op verschillende manieren niet voldoende is. Het is ook nodig om medewerkers te trainen in de nieuwe wet- en regelgeving en bewustwordingscampagnes in te zetten. Ook gebouwrondes kunnen helpen bij het creëren van bewustwording van medewerkers, omdat ze op deze manier zien dat de regels gehandhaafd worden. In een grote organisatie is het wellicht handig een ambassadeurssessie te organiseren en van elke afdeling iemand als privacyambassadeur in te zetten. Zo hoeft de organisatie niet elke medewerker apart te informeren, maar kunnen de privacyambassadeurs het onderwerp onder de aandacht

brengen en houden op hun afdeling. Herhaling en variatie zijn sleutelwoorden bij communicatie. Niet iedereen neemt informatie op dezelfde manier tot zich, dus hou hier rekening mee bij het organiseren van de interne communicatie.

5. Stel duidelijke procedures op voor het behandelen van beveiligingsincidenten en communiceer hierover

Om beveiligingsincidenten te behandelen moeten in een zorginstelling duidelijke procedures aanwezig zijn. Zo moet bijvoorbeeld duidelijk zijn wie waarvoor verantwoordelijk is en wanneer er een melding moet worden gedaan bij de Autoriteit Persoonsgegevens. Daarom is het belangrijk om dit vast te leggen en duidelijk te communiceren naar de organisatie. Dit kan op dezelfde manier als gecommuniceerd wordt over het informatiebeveiligingsbeleid. Zorg in ieder geval dat medewerkers weten waar ze een melding kunnen doen en betrek medewerkers ook in het proces door terug te koppelen aan hen wat er met de meldingen gebeurd is.

6. Evalueer regelmatig het informatiebeveiligingsbeleid en pas het beleid indien nodig aan

Om het informatiebeveiligingsbeleid up-to-date te houden is het van belang continu te kijken naar verbeterpunten in het beleid. Zeker met de komst van de Algemene Europese Verordening is het van belang de privacywet- en regelgeving continu te checken en te kijken of er nog steeds in lijn met deze wetgeving gehandeld wordt.

6. Discussie

In deze sectie zullen eerst de geformuleerde adviezen worden besproken en hun verhouding tot de literatuur over interne communicatie, waarna zal worden ingegaan op de toepasbaarheid van de adviezen voor de zorgsector, de beperkingen van het onderzoek en mogelijke suggesties voor vervolgonderzoek.

6.1 Samenhang van adviezen met literatuur

Het eerste geformuleerde advies is het zorgen voor actieve betrokkenheid van het bestuur. Eén van de functies van interne communicatie is volgens Vos en Schoemaker (2011) het bevorderen van de betrokkenheid. Ook geven Vos en Schoemaker aan dat motivatie ontstaat als iemand zich persoonlijk betrokken voelt bij een onderwerp. Het zou dus goed kunnen dat het betrekken van het bestuur bij het privacythema leidt tot meer motivatie van het bestuur om conform de nieuwe privacywet- en regelgeving te handelen.

Bovendien werd aangegeven dat er meer verantwoordelijkheid van het bestuur komt met de Algemene Verordening Gegevensbescherming die in 2018 handhaafbaar wordt. Ook moet een bestuur aan kunnen tonen met documenten dat zij accountable is met de nieuwe wetgeving. Daarom lijkt het een logisch gevolg dat het bestuur ook een actieve rol moet spelen bij de invulling van de nieuwe privacywet- en regelgeving.

Ook kan het realiseren van actieve betrokkenheid helpen bij het doorvoeren van een verandering. Zolang bestuursleden actief betrokken zijn bij het beleid, hebben zij meer gevoel voor de manier waarop medewerkers tegen de problematiek aankijken en kunnen zij hun beleid hier beter op laten aansluiten. Er is daardoor een grotere kans om in de Goldilock's zone te komen (Clampitt, 2013). Ook kunnen bestuursleden door hun betrokkenheid de verschillende reacties van medewerkers beter begrijpen, waardoor er minder kans is op weerstand tegen de verandering (Clampitt, 2013).

Verder toont de actieve betrokkenheid van het bestuur een goed voorbeeld voor andere medewerkers om zich aan de nieuwe privacywet- en regelgeving te houden. Hierdoor wordt ingespeeld op de waargenomen norm van medewerkers (Fishbein & Ajzen, 2011)

Het tweede geformuleerde advies is het zorgen voor prioriteit van privacy in de organisatie. Vos en Schoemaker geven aan dat medewerkers gemotiveerd moeten zijn voor de veranderingen en bereid moeten zijn zich in te zetten om een verandering tot stand te brengen (2011). Als een onderwerp een lage prioriteit krijgt in de organisatie, dan zal dit niet leiden tot motivatie van medewerkers. Het geven van een hoge prioriteit aan privacy door bijvoorbeeld het onderdeel maken van functioneren van een werknemer of door budget ervoor vrij te maken als organisatie laat zien dat de organisatie het thema belangrijk vindt wat bijdraagt aan een stimulerend klimaat voor medewerkers om zich in te zetten voor de verandering (Winkelman, 2015).

Het derde geformuleerde advies is het in kaart brengen van beveiligingsrisico's en het opstellen van een informatiebeveiligingsbeleid op basis hiervan. Dit advies heeft minder direct verband met de theorieën die zijn besproken. Het hebben van een informatiebeveiligingsbeleid is een minimale voorwaarde om hierover te kunnen communiceren. Het informatiebeveiligingsbeleid opstellen aan de hand van beveiligingsrisico's is een voorwaarde die de wet stelt aan het informatiebeveiligingsbeleid. Dit maakt dit advies meer tot een voorwaarde dan tot een discussiepunt.

Het vierde geformuleerde advies bestaat uit het communiceren over het informatiebeveiligingsbeleid en het werken aan beveiligingsbewustzijn. Door te communiceren over het informatiebeveiligingsbeleid worden mensen op de hoogte gesteld van gewenste veranderingen. Daarmee wordt voldaan aan de kennisdoelstellingen bij een verandering, die Vos en Schoemaker (2011) formuleerden. Het werken aan het beveiligingsbewustzijn kan gezien worden als methode om de medewerkers te motiveren voor de verandering en ervoor te zorgen dat zij bereid zijn zich voor de verandering in te zetten (Vos & Schoemaker, 2011). Met een bewustwordingscampagne kan bijvoorbeeld worden ingezet op het veranderen van de attitude van de medewerker ten opzichte van het naleven van de privacywet- en regelgeving (Fishbein & Ajzen, 2011).

Het vijfde geformuleerde advies bestaat uit het opstellen van duidelijke procedures en het communiceren hierover. Het communiceren over de procedures draagt eveneens bij aan de kennisdoelstellingen bij een verandering, die Vos en Schoemaker formuleerden.

Het zesde geformuleerde advies bestaat uit het regelmatig evalueren en aanpassen van het beleid. Dit lijkt een logische stap, aangezien de privacywet- en regelgeving continu aan verandering onderhevig is. De technologie ontwikkelt zich voortdurend, waardoor de eisen aan privacy in de toekomst alleen nog maar strenger zullen worden.

6.2 Toepasbaarheid adviezen zorgsector

De adviezen uit de conclusie zijn gebaseerd op bestaande richtlijnen voor zorginstellingen en op gesprekken met functionarissen voor de gegevensbescherming en experts. De bestaande richtlijnen voor zorginstellingen zorgden voor een breder kader, waar de interviews zorgden voor een specifiekere invulling van deze kaders. De brede kaders en de breed geformuleerde adviezen zullen goed toepasbaar zijn op zorginstellingen, aangezien deze voortkomen uit de richtlijnen van bestaande privacywet- en regelgeving. Er kunnen hier wel uitzonderingen op bestaan. Zo bleek bijvoorbeeld dat het bestuur van een UMC niet actief betrokken is bij het uitvoeren van het privacybeleid, maar dat een UMC ondanks het gebrek aan actieve betrokkenheid van het bestuur, wel goede invulling kan geven aan de overige communicatierichtlijnen. Het is dus ook afhankelijk van de al aanwezige organisatiecultuur of actieve betrokkenheid van het bestuur vereist is.

De manier waarop invulling gegeven wordt aan de geformuleerde adviezen kunnen verschillen per instelling. Dit bleek al uit de hoeveelheid manieren om invulling te geven aan de communicatierichtlijnen die uit de interviews voortkwamen. Hierin zullen zorginstellingen zelf een keuze moeten maken wat voor hen wel of niet werkt. Dit is ook geheel afhankelijk van het budget dat zorginstellingen beschikbaar hebben en de aanwezige communicatiecultuur. Niet voor niets geeft de wetgeving aan dat een organisatie passende maatregelen moet treffen.

6.3 Beperkingen van het onderzoek

De grootste beperking van het onderzoek is dat er interviews zijn afgenomen met maar twaalf zorginstellingen, terwijl er in totaal rond de 862 zorginstellingen in Nederland zijn. De invulling van de communicatierichtlijnen door deze zorginstellingen, hoeven daarom niet van toepassing te zijn op alle zorginstellingen in Nederland. Het kan voorkomen dat sommige manieren van invulling van de interne communicatie voor ziekenhuizen wel goed werken, maar voor bijvoorbeeld GGZ-instellingen niet. Toch bleken de manieren van communicatie die genoemd werden door zorginstellingen veelal hetzelfde en lijkt de interne communicatie wel in te vullen op basis van de antwoorden op de hoofdvraag.

De vastgestelde communicatierichtlijnen komen voort uit de richtlijnen die gebaseerd zijn op de huidige privacywet- en regelgeving voor de gehele zorgsector, waardoor deze gemakkelijk toepasbaar zouden moeten zijn op de gehele sector. Dit bleek ook uit de interviews. De geïnterviewde zorginstellingen konden namelijk voldoende voorbeelden geven van hoe zij invulling gaven aan deze richtlijnen. Hier moet echter wel bij vermeld worden dat er specifiek is gezocht naar zorginstellingen die al bezig waren invulling te geven aan dit thema, zodat antwoord geformuleerd kon worden op de hoofdvraag van dit onderzoek. Er zijn ook genoeg zorginstellingen in Nederland nog niet bezig met het invullen van de privacywet- en regelgeving voor hen is het wellicht lastiger de communicatierichtlijnen toe te passen.

Een andere beperking van het onderzoek is dat de adviezen specifiek gericht zijn op de zorgsector en wellicht minder toepasbaar zijn op andere sectoren die ook te maken hebben met de nieuwe privacywet- en regelgeving. De adviezen zijn wel deels gebaseerd op de algemene CBP-richtsnoeren die voor alle sectoren van toepassing zijn. Ook zijn de adviezen zo algemeen geformuleerd dat ze gemakkelijk vertaald kunnen worden naar andere sectoren. Enkel de invulling van het interne communicatiebeleid kan verschillen van die van de zorgsector. De voorbeelden van communicatiemiddelen die genoemd zijn in dit onderzoek zijn wellicht minder toepasbaar voor andere sectoren. Dit zou echter geen probleem hoeven te vormen als de organisatie beschikt over een goede eigen communicatieafdeling. Deze zou vanuit de opgestelde communicatierichtlijnen gebaseerd op de wetgeving gemakkelijk een vertaalslag moeten kunnen maken naar het eigen interne communicatiebeleid. Dit onderzoek geeft daarbij goede richtlijnen voor het inrichten van het interne communicatiebeleid, maar de organisatie moet altijd zijn eigen cultuur en werknemers in gedachte houden bij het vormgeven van beleid. Dit onderzoek gaf met name aan hoe groot de rol van communicatie kan zijn bij dit thema en dat zorginstellingen dit niet moeten onderschatten.

6.4 Suggesties voor vervolgonderzoek

Dit onderzoek was een eerste onderzoek in de zorgsector naar dit thema. Een logische vervolgstap zou zijn om te toetsen in hoeverre de zorginstellingen de communicatierichtlijnen opvolgen. Dit onderzoek zou inzicht kunnen geven op de status van zorginstellingen en in hoeverre zij al in lijn met de nieuwe privacywet- en regelgeving opereren. Dit onderzoek kan kwantitatief zijn van aard, omdat de communicatierichtlijnen al geformuleerd zijn en de genoemde invullingen van deze richtlijnen gebruikt kunnen worden als scores, waarbij de zorginstelling punten kan scoren op de verschillende richtlijnen en manieren van invulling. Hierbij geldt

bijvoorbeeld voor het tonen van actieve betrokkenheid dat aan hoe meer punten een zorginstelling hier voldoet hoe meer het actieve betrokkenheid toont. Voor het communiceren van beleid en het verhogen van bewustzijn zijn herhaling en variatie sleutelwoorden. Er kan gekeken worden van welke manieren zorginstellingen gebruik maken en als variatie en herhaling hier een rol speelt dan kan een zorginstelling hier een hogere score op krijgen, dan wanneer dit geen rol speelt.

Een vervolgonderzoek dat hierop aansluit zou kunnen zijn dat ook medewerkers in de organisatie bevraagd worden wat zij van het huidige interne communicatiebeleid omtrent dit thema vinden en in hoeverre zorginstellingen zich hierin nog zouden kunnen verbeteren. De geformuleerde richtlijnen zouden de thema's kunnen vormen van de enquête waarover een aantal vragen gesteld kunnen worden aan de medewerkers. De vervolgonderzoeken krijgen daarmee een meer toetsend karakter, waardoor de zorgsector zich binnen dit thema verder kan ontwikkelen.

Bovendien is de bespreking van de resultaten in dit onderzoek gebaseerd geweest op de communicatierichtlijnen die geformuleerd waren uit de documentanalyse. Er is tijdens de interviews naast over deze onderwerpen ook nog over andere onderwerpen gesproken, zoals bijvoorbeeld de rol van de Autoriteit Persoonsgegevens. Deze onderwerpen waren voor het beantwoorden van de onderzoeksvraag minder relevant, maar zijn voor het begrip van hoe zorginstellingen op dit moment in dit thema staan wel interessant. Deze resultaten kunnen gebruikt worden wanneer de geformuleerde adviezen geïmplementeerd worden in de zorgsector.

Literatuurlijst

Algemene Verordening voor de Gegevensbescherming (2016) geraadpleegd op 18-12-2016 via https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/verordening_2016_-_679_definitief.pdf

Agre P.E., Rotenberg M. (2001), *Technology and Privacy: The New Landscape.* MIT Press: Cambridge, Massachusetts

Autoriteit Persoonsgegevens (2015, 30 december), De meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp) Beleidsregels. Geraadpleegd op 22-08-2016 via https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/richtsnoeren_meldplicht_datalekken.pdf

Autoriteit Persoonsgegevens (2016), Belangrijkste bepalingen Wbp. Geraadpleegd op 09-12-2016 via https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/wet-bescherming-persoonsgegevens

Autoriteit Persoonsgegevens (2016), Meldplicht datalekken. Geraadpleegd op 14-01-2017 via https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken

Autoriteit Persoonsgegevens (2017), Functionaris voor de gegevensbescherming. Geraadpleegd op 14-01-2017 via https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/functionaris-voor-de-gegevensbescherming

College Bescherming Persoonsgegevens (2013), Richtsnoeren CBP: Beveiliging van Persoonsgegevens. Geraadpleegd op 06-12-2016 via https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf

Centraal Bureau voor de Statistiek (2016), Zorginstellingen; kerncijfers, financiën en personeel. Geraadpleegd op 14-01-2017 via http://statline.cbs.nl/StatWeb/publication/?VW=T&DM=SLNL&PA=81451NED&LA=NL

Clampitt, P. (2013). Communicating for Managerial Effectiveness. Problems. Strategies. Solutions. Thousand Oaks, London: Sage.

Deloitte (2016), Cyber Security of network connected medical devices in (EMEA) hospitals 2016. Rapport opgevraagd via Deloitte.

Fishbein, M., & Ajzen, I. (2011). *Predicting and changing behavior: The reasoned action approach*. Taylor & Francis.

Hoeken, H., Hornikx, J. & Hustinx, L. (2012). Overtuigende teksten. Onderzoek en ontwerp. Bussum: Uitgeverij Coutinho.

ISO-27001 (2005) Information technology – security techniques – code of practice for information security management. Geraadpleegd op 06-12-2016 via http://www.slinfo.una.ac.cr/documentos/EIF402/ISO27001.pdf

Martijn, M. & Tokmetzis, D. (2016) Je hebt wél iets te verbergen. *Over het levensbelang van privacy.* De Correspondent

NEN-7510 (2011) Werken met de NEN-7510. Geraadpleegd op 06-12-2016 via https://www.werkenmetnen7510.nl/publicaties/nen-7510-2011/sec_3

NRC (2016, 28 december) Meeste melding van datalekken uit zorgsector. Geraadpleegd op 15-01-2017 via https://www.nrc.nl/nieuws/2016/12/28/meeste-melding-van-datalekken-uit-zorgsector-5934186-a1538645

NU.nl (2016, 29 december) Gegevens van 1400 UMCG-patiënten gelekt na diefstal laptops. Geraadpleegd op 15-01-2017 via http://www.nu.nl/tech/4372091/gegevens-van-1400-umcg-patienten-gelekt-diefstal-laptops.html

NU.nl (2016, 06 oktober) Patiëntgegevens Isala ziekenhuis op straat na diefstal laptops. Geraadpleegd op 15-01-2017 via http://www.nu.nl/binnenland/4332366/patientgegevens-isala-ziekenhuis-straat-diefstal-laptop.html

NU.nl (2016, 25 januari) Datalek ziekenhuizen treft ruim 200.000 patiënten. Geraadpleegd op 15-01-2017 via http://www.nu.nl/internet/4203392/datalek-ziekenhuizen-treft-ruim-200000-patienten.html

Oelen, U. (2016), Ronde tafelbijeenkomst meldplicht datalekken van de NGFG.

PwC Nederland (2015), Privacy Governance Onderzoek: Volwassenheid van privacybeheersing binnen Nederlandse organisaties. Geraadpleegd op 24-08-2016 via http://www.pwc.nl/nl/assets/documents/pwc-privacy-governance-onderzoek-2016.pdf

Verizon (2016), Data Breach Investigations Report. *Understand what you're up against.* Geraadpleegd op 20-09-2016 via http://www.verizonenterprise.com/verizon-insights-lab/dbir/

Vos, M., & Schoemaker, H. (2011). Geïntegreerde communicatie. *Concern-, interne en marketingcommunicatie*. Boom Koninklijke Uitgevers

Warren, S. & Brandeis, L. (1890), The right to privacy. *Harvard Law Review,* IV, 5.

Westin, A.F. (1968), Privacy and freedom. *Washington and Lee Law Review*, 25, 1.

Winkelman (2015), Model voor inrichting interne communicatie. Geraadpleegd via Winkelman en Van Hessen

Zandvliet (2016), Security in de zorg vraagt om stapsgewijze aanpak. *Zorg en ICT.* Geraadpleegd op 24-08-2016 via http://www.zorg-en-ict.nl/newsitem/20204

Masterscriptie Bijlagen

Communicatie en Organisatie

Sharing is caring?

Kwalitatief onderzoek naar de manier waarop zorginstellingen hun interne communicatie over privacybescherming en informatiebeveiliging inrichten om te kunnen opereren conform de nieuwe privacywet- en regelgeving

Bronnen: NRC en NU.nl (2016)

Student: Renske Swarts

Studentnummer: 5622328

E-mail: renskeswarts@gmail.com

Docent: dr. Hanny den Ouden

Tweede lezer: dr. Ingeborg van der Geest

Stagebegeleiders Winkelman en Van Hessen:

Michel van Schie

Sharon McIntosh

Datum: 16-01-2017

Universiteit Utrecht

Inhoudsopgave

Bijlage 1 Privacyverklaring zorginstellingen

Privacyverklaring

Onderzoeksvraag: Hoe is de interne communicatie van zorginstellingen omtrent de bescherming van persoonsgegevens geregeld?

Verantwoordelijke onderzoeker: Renske Swarts

Opleiding: Master Communicatie en Organisatie Universiteit Utrecht

Hoe worden de onderzoeksgegevens verwerkt?

Alle besproken gegevens zullen geanonimiseerd verwerkt worden. Dit betekent dat quotes uit interviews bijvoorbeeld als volgt zullen worden weergegeven: Privacy Officer van zorginstelling x zegt hierover: "…" (hierin wordt indien relevant wel onderscheid gemaakt tussen ziekenhuizen en GGZ-instellingen, zodat mogelijke verschillen in aanpak tussen beide soort instellingen duidelijk analyseerbaar zijn).

Indien er namen in het interview worden genoemd, zullen deze niet overgenomen worden in de uitwerking van het interview. Een ieder die het onderzoeksrapport leest, zal enkel de geanonimiseerde versie van het interview te zien krijgen. Er zal dus niet herleidbaar zijn van welke zorginstelling welk interview afkomstig is.

Ter bevordering van het verwerken van de gegevens zal het interview worden opgenomen. De opnames zullen enkel gebruikt worden om de informatie gemakkelijk te kunnen verwerken. Tijdens het uittypen van de informatie zullen de gegevens direct geanonimiseerd worden. De opnames zullen tot de oplevering van het onderzoeksrapport door de onderzoeker bewaard worden in een beveiligde map waar enkel de onderzoeker toegang tot heeft. Na oplevering van het onderzoeksrapport zullen de opnames worden verwijderd.

Datum: Handtekening deelnemer: Handtekening onderzoeker:

Bijlage 2 Topiclijst interviews zorginstellingen

1. De Functie van Functionaris voor de Gegevensbescherming
- -Achtergrond van de Functionaris voor de gegevensbescherming
- -Informatie over de instelling
- -Taken en verantwoordelijkheden
- -Verhouding tussen privacy en de bescherming van persoonsgegevens

2. **De belegging van de functie in de organisatie**
- -Plek afdeling
- -Samenwerking met andere afdelingen
- -Samenwerking met Raad van Bestuur

3. Informatiebeveiligingsbeleid
- -Verantwoordelijkheid opstellen/uitvoeren beleid
- -Inrichting beleid
- -Maatregelen bij niet naleven regels
- -Lastige punten om beleid door te voeren

4. Communicatie over informatiebeveiligingsbeleid
- -Inzet van communicatie
- -Lastige groepen om te bereiken
- -Verschillende benaderingswijze voor verschillende groepen
- -Bekendheid met 'ZEKER' campagne
- -Bewustwordingscampagnes
- -Evaluatie van beleid

5. Gevolgen van datalek
- -Risico's op datalek
- -Risico's in beeld bij bestuur
- -Bijdrage van communicatie om risico's in te perken

6. Betrokkenheid van bestuur
- -Thema in beeld bij bestuur
- -Voorbeelden waaraan je betrokkenheid kunt zien

7. Prioriteit van privacy in de organisatie
- -Hoge of lage prioriteit
- -Waaraan kun je dit zien?

8. Meldplicht Datalekken
- -Veranderingen in organisatie sinds Meldplicht Datalekken
- -Procedure Meldplicht Datalekken
- -Rol van de Autoriteit Persoonsgegevens
- -Voorbereiding op de AVG

9. Communicatie over Meldplicht Datalekken

Bijlage 3 Codeerschema interviews zorginstellingen

1. **Functie van de Functionaris voor de Gegevensbescherming**
   -Achtergrond van de Functionaris voor de Gegevensbescherming
   -Belegging van de functie in de organisatie
   -Informatie over de instelling
   -Verhouding tussen privacy en de bescherming van persoonsgegevens

2. **Informatiebeveiligingsbeleid**
   -Inrichting van informatiebeveiligingsbeleid
   -Wie stelt beleid op
   -Beveiligingsmaatregelen
   -Maatregelen bij niet naleven regels
   -Lastige punten om beleid door te voeren

3. **Communicatie over informatiebeveiligingsbeleid**
   -Communicatie-inzet informatiebeveiligingbeleid
   -Lastige groepen om te bereiken
   -Verschillende benaderingswijze voor verschillende groepen
   -Bekendheid met 'ZEKER' campagne
   -Informatie voor patiënten
   -Welke methode werkt wel en welke methode werkt niet

4. **Risico-inventarisatie**
   -Risico's voor instelling van een datalek
   -Bijdrage van communicatie om risico's in te perken

5. **Betrokkenheid van bestuur**
   -Risico's in beeld bij bestuur
   -Thema in beeld bij bestuur

6. **Prioriteit van privacy in de organisatie**

7. **Beveiligingsbewustzijn in de organisatie**
   -Aandacht van medewerkers voor thema
   -Awareness vergroten
   -Motivatie van medewerkers om te gaan melden
   -Bewustzijn van medewerkers
   -Vragen van medewerkers

8. **Meldplicht Datalekken**
   -Veranderingen in organisatie sinds Meldplicht Datalekken
   -Procedure Meldplicht Datalekken
   -Meldingen

9. **Communicatie-inzet naar aanleiding van Meldplicht Datalekken**

10. **Evaluatie**
    -Evaluatie van beleid
    -Evaluatie van incidenten

11. **Rol van externe partijen**
    -Rol van de Autoriteit Persoonsgegevens
    -Regionale samenwerkingen
    -Relatie met de gemeente

-Twee toezichthouders: IGZ en AP
-Bijeenkomst van de NGFG

12. **Voorbereiding op de AVG**

13. **Samenwerking met communicatieafdeling**

14. **Zorginstelling specifieke voorbeelden**
-Voorbeeld van niet-officiële communicatiemethode die goed werkt (methode die werkt om bewustwording te vergroten)
-Voorbeeld: in combinatie moeilijker om persoonsdata te herkennen
-Voorbeeld van het plascontract
-Voorbeeld van audit door GGD
-Voorbeeld van incident
-Voorbeeld radiologievoorlichting

Bijlage 4 Uitwerking interviews experts

Bijlage 4.1 Uitwerking interview Cure4

Marieke van Dijk & Ilham Ouajnan

RS: Eerst benieuwd wat jullie hier precies doen natuurlijk.

MVD: Ik ben de manager van de Business Line Legal bij Cure4 en in het kader daarvan adviseren wij zorginstellingen op het gebied van privacy, maar ook aan de zorg gerelateerde ondernemingen, zoals ICT-leveranciers en gemeentes met een zorgtaak. We geven naast advies ook trainingen en seminars. Met trainingen ondersteunen we bijvoorbeeld onze opdrachtgevers ook procesmatig. Dus we geven niet alleen adviezen, maar we helpen ook bij de implementatie daarvan. Dat is kort in een notendop hoe onze dienstverlening eruit ziet op het gebied van privacy. Naast Privacy Officer voor zorginstellingen, zijn wij ook privacy- en compliance officers binnen de groep, maar dat is voor dit onderwerp minder relevant.

RS: Ja, want met wat voor soort zorginstellingen werken jullie dan samen?

MVD: De GGZ, dat is eigenlijk de belangrijkste groep.

IO: Maar in feite met alle.

MVD: Ja, in feite met alle.

RS: En hier in de regio Utrecht met name?

IO: Nee, dat is echt wel landelijk.

MVD: Ja, precies. En de doelgroep dat zijn voornamelijk de instellingen die eigenlijk te klein zijn om zelf een privacy officer aan te stellen. De grote ziekenhuizen die zijn natuurlijk groot genoeg om iemand daar fulltime op te zetten en onze doelgroep zijn de instellingen die het allemaal wel geregeld moeten hebben, die ook een privacy officer moeten hebben, maar daar gewoon geen FTE's voor vrij kunnen maken en daarom bieden wij het ook als een service aan in een flexibele abonnementsvorm, zodat je afhankelijk van de grootte van je organisatie kunt bepalen voor hoeveel uur per maand je het abonnement bij ons wilt afnemen.

RS: Ja, dus ze kunnen zelf eigenlijk kiezen hoeveel uur er nodig is in overleg met jullie en vanuit daar wordt de functie ingevuld. En hoe doen jullie dat dan? Want jullie zitten waarschijnlijk extern. Hoe zit die samenwerking in elkaar?

IO: Wij zitten ook wel veel bij de klant inderdaad. Dat is een beetje afhankelijk van het aantal dagdelen dat bij ons afgenomen wordt en de geformuleerde projecten, die op dat moment lopen. Het is namelijk afhankelijk van de vragen die er op dat moment zijn, welke projecten er zijn geformuleerd en of daarvoor nodig is dat je veel contact maakt bij de klant zelf op locatie of dat het nodig is dat je veel moet uitwerken. Indien uitwerking nodig is doen we dat op kantoor als we daar de klant niet voor nodig hebben.

MVD: Ja, je ziet het is wel belangrijk om bij de klant aanwezig te zijn. Het is namelijk van belang dat we zien wat er op de werkvloer gebeurt.

IO: Ja, je krijgt veel meer feeling ook dan en meer inzicht in alle processen bij de klant.

MVD: Je moet echt goed feeling krijgen bij het type organisatie, type mensen en waar de problematiek ligt. Dus inderdaad ons werkconcept is echt dat we het niet vanuit hier alleen doen.

RS: Want de functie van privacy officer is natuurlijk vrij nieuw en ook vrij breed nog op dit moment in te vullen. Welke dingen doen jullie dan met name voor die zorginstellingen? Wisselt dat heel erg of zit er wel vaak een lijn in?

MVD: De start wisselt heel erg. Je ziet bepaalde organisaties willen eigenlijk in eerste instantie snel bepaalde zaken op orde hebben: scan onze bewerkersovereenkomsten, help ons met een protocol van datalekken bijvoorbeeld. Sommige organisaties zijn nog helemaal aan het begin en die wensen bijvoorbeeld eerst een QuickScan van de organisatie zodat ze weten waar ze staan. Op basis van de bevindingen maken we dan een plan met projecten die we verder in gaan vullen. Dus ja dat varieert van organisatie tot organisatie en is afhankelijk van wat er binnen de organisatie reeds op orde is en waar er nog behoefte is aan ondersteuning, of ondersteuning nodig is om compliant te zijn.

RS: Ja dus dat kan heel erg verschillen, want als jullie bij zo'n instelling komen is er dan over het algemeen al wel iets van een privacybeleid opgesteld?

MVD: Ook dat verschilt heel erg, maar meestal niet. Soms is er wel iets geregeld of opgesteld. Dan is er bijvoorbeeld vanuit kwaliteitsoogpunt aandacht aan besteed.

IO: Indien organisaties zijn gecertificeerd, zie jij bijvoorbeeld ook dat er het één en ander geregeld is, maar dit is vaak niet voldoende.

RS: Nou ja, dat is ook de reden waarom ze waarschijnlijk bij jullie aankloppen. Als ze alles geregeld hadden, dan hadden ze niemand nodig natuurlijk. En je hebt natuurlijk privacy en je hebt de bescherming van persoonsgegevens: hoe staan die twee in verhouding volgens jullie?

IO: Ja, privacy is eigenlijk een grondrecht natuurlijk dat is opgenomen in de grondwet en internationale verdragen, maar in de volksmond is privacy de bescherming van persoonsgegevens.Dat zijn twee verschillende dingen natuurlijk. Wij werken vanuit de Wet Bescherming Persoonsgegevens en de Europese Privacy Verordening en alle andere regelgeving die van toepassing is op de bescherming van persoonsgegevens. Maar privacy en de bescherming van persoonsgegevens zijn voor ons één. In die zin dat als we het hebben over privacy dan hebben we het eigenlijk over de bescherming van persoonsgegevens.

RS: Oké en vanuit de instellingen worden er dan mensen bij betrokken die bij de instellingen werken?

IO: Dat is ook wel wisselend, want we zijn nu bij een aantal zorginstellingen en zorggerelateerde bedrijven ingezet en het varieert van organisatie tot organisatie. Bij de één krijg je echt de autonomie om zelf aan te geven welke stappen er nodig zijn en stel je zelf een plan van aanpak op, maar bij de andere worden interne medewerkers gekoppeld aan de projecten, die gezamenlijk met ons de projecten formuleren en hun medewerkers hieraan koppelen, zodat het geheel intern geborgd wordt, zoals de know-how waarin wij voorzien.

MVD: Wij vinden het belangrijk om aansluiting te zoeken bij de organisatie, bijvoorbeeld een applicatiebeheerder, of iemand vanuit het bestuur, want wij zijn juristen met een ICT-achtergrond, dus dat stuk kunnen we ook wel beoordelen, maar het teamwork binnen de organisatie kunnen wij niet alleen invullen en is wel echt belangrijk. Dit is bijvoorbeeld van belang voor de adviezen die wij geven en de protocollen die wij uitwerken. Deze moeten geborgd worden in de organisatie, naast dat ze geimplementeerd moeten worden. Als we dat in ons eentje opstellen, zonder back-up vanuit de organisatie, dan krijg je het niet voor elkaar.

RS: Nee, dan krijg je het niet doorgevoerd, dat zie je bij ons ook natuurlijk. Maar wie haal je er dan uit zo'n organisatie bij het liefste?

MVD: Nou in ieder geval iemand vanuit het bestuur, want er moet op het gebied van privacy natuurlijk altijd gerapporteerd worden aan het bestuur, dus die back-up is enorm belangrijk. Maar vaak zie je ook dat iemand of vanuit de facilitaire hoek, vanuit ICT of vanuit het kwaliteitsbeheer aanhaakt.

RS: Ja, en op het gebied van communicatie gebeuren daar ook dingen?

MVD: Nee, nog niet. En dat is iets wat wij ook vaak wel aan de orde stellen.

– onderbreking van het gesprek vanwege verplaatsing naar andere zaal-

-Gesprek hervat-

MVD: Communicatie is vaak niet aan gedacht en dat is wel vaak wat wij naar voren brengen, wat echt wel onderdeel is als wij een project aanvliegen. Daarin zit een stuk technisch, een stuk juridisch en een stuk communicatie dat we dan naar voren brengen. Op het moment dat je de communicatie goed optuigt dan kun je het probleem klein houden, als je dat niet doet dan kan het probleem heel erg uit de hand lopen en dat is niet wenselijk.

RS: Maar hebben ze vaak ook iemand van communicatie op die GGZ-instellingen?

MVD: Nee.

RS: Nee, daar hebben ze ook vaak niet iemand voor, dat is dan ook een lastig punt.

MVD: Meestal de communicatie dat is dus eigenlijk de bestuurder hè die naar buiten toe communiceert, maar of die nou ook echt aan crisismanagement doet en dat in de communicatie meeneemt, dat is de vraag.

RS: Ja, Medewerkers dat is natuurlijk een hele belangrijke groep. Ik geloof ongeveer 80% van de datalekken komt door menselijke fouten, dus belangrijk in ieder geval. Wat voor gevolgen van zo'n datalek issue denken jullie dat belangrijk wordt gevonden in de zorginstellingen?

IO: Oh, de boetes. De boetes zijn wel een heikel punt, maar ook het imago van de organisatie. Dus daar speelt communicatie een grote rol bij. Maar wat wel leuk is om te vertellen: wij voorzien klanten van bijvoorbeeld verschillende protocollen en daarbij denken wij dus ook aan communicatie door een communicatieprotocol op te stellen in relatie tot bijvoorbeeld datalekken, zodat naar buiten toe in elk geval in één lijn wordt gecommuniceerd en daar weloverwogen een standpunt in genomen wordt door de medewerkers binnen de organisatie die daarover moeten beslissen.

RS: Ja, en wat staat er dan bijvoorbeeld in zo'n protocol?

MVD: Dat bijvoorbeeld alle telefoontjes die bij de receptie binnenkomen direct doorgeleid worden naar de persoon die het woord mag voeren. Dat medewerkers alle informatie die ze binnenkrijgen ook naar die persoon doorsturen. Eigenlijk wordt er één centraal persoon aangewezen die de communicatie doet, die de pers te woord staat of die eventueel andere publicaties op de website coördineert, maar met name dat er met één mond gesproken wordt.

RS: Ah, oké dus dat gaat meer om de externe communicatie bijvoorbeeld als er een datalek voorkomt.

IO: Ja, maar ook de interne hoor. Interne communicatie wordt hier ook in meegenomen, maar de externe is vooral belangrijk, omdat deze vergaande gevolgen kan hebben voor het imago of de reputatie van de organisatie.

RS: Ja, want wat staat daar dan bijvoorbeeld in voor intern?

MVD: Nou, intern is belangrijk, maar dan is het niet zozeer de communicatie als er een datalek heeft plaatsgevonden, maar meer daaraan voorafgaand. Een stroomlijn zodat als mensen dingen ontdekken ze weten bij wie ze dat moeten melden, hoe ze dat moeten melden en dat ze eventueel aanvullende informatie kunnen aangeven, zodat bijvoorbeeld medewerkers niet zelf gaan oordelen of er sprake is van een datalek of niet, maar dat ze alle securityincidenten waar ze mee te maken krijgen melden en dat er dan een datalekteam

is dat daar verder dan wel over na gaat denken. Dus eigenlijk de boodschap is een beetje: meld vooral alles wat je tegenkomt en denk niet zelf na, want dan heb je kans dat er heel veel een eigen leven gaat leiden, dus we proberen alles zo centraal mogelijk te regelen.

IO: En als je dan meldt om dat dan zo zorgvuldig mogelijk te doen, in alle lijnen gedacht. Dus bijvoorbeeld naar het bestuur toe en naar andere collega's. Dat er geen paniek gezaaid wordt als dat bijvoorbeeld helemaal niet nodig is en dat er dan bijvoorbeeld niet een heel ander verhaal naar buiten komt, omdat het intern niet goed geregeld is. Dat stukje bewustwording/awareness is vooral van belang en nemen wij in al onze projecten enorm serieus.

RS: Ja, want hoe wordt het dan doorgevoerd in zo'n organisatie? Jullie maken een plan op voor zo'n organisatie, zien jullie daar dingen van terug? Blijven jullie dan nog een tijdje bij die organisatie hangen?

MVD: Het is onderdeel van ons totale proces eigenlijk. En onderdeel van ons totale privacyproject om de hele organisatie 'privacyproof', 'privacycompliant' te maken. Dit hele verhaal hebben we bijvoorbeeld verwerkt in ons stappenplan rondom datalekken. Daar blijven we als privacy officers bij betrokken zodat we ook bij kunnen sturen en ondersteunen op het moment dat zich een incident voordoet.

RS: En zou je dan zeggen dat in de organisaties waarvoor jullie werken privacy een hoge prioriteit heeft of een lage?

MVD: Nou je merkt, de organisaties waar wij voor werken, daar wordt de prioriteit steeds hoger.

RS: Ja, en waaraan kan je dat bijvoorbeeld zien?

MVD: Op het moment dat we aan de slag gaan, op het moment dat we één keer een training hebben gegeven en gaan starten. Dan komen er ineens heel veel dingen naar boven in de organisatie. Medewerkers worden meer betrokken, omdat ze ook beter geïnformeerd zijn . Ze stellen bijvoorbeeld zelf meer kritische vragen zoals "Hee ik heb nu hiermee te maken is dit misschien een datalek?" Of "Mag ik dit wel of niet mailen?" En dat krijgen we inderdaad ook terug vanuit vanuit de bestuurders. Medewerkers worden ineens wakker. En dan zie je de prioriteit ook stijgen.

RS: Ja, want er worden dus trainingen gegeven aan de medewerkers ook. Aan alle medewerkers van die instelling of bepaalde groepen wordt daar onderscheid in gemaakt?

IO: Afhankelijk van hoe de klant dat wil, maar in feite is het wel wenselijk dat je alle medewerkers mee kunt nemen.

RS: Ja, ik kan me voorstellen dat het wel lastig is bij GGZ-instellingen, omdat je ook heel veel mensen hebt op de werkvloer zoals bijvoorbeeld huishoudelijke hulpen.

MVD: Meestal worden er dan gewoon groepjes gemaakt. Je kunt ook het principe hanteren: je doet een bepaalde groep medewerkers die dat dan vervolgens weer meenemen in de organisatie naar medewerkers die onder hen werken. Dat kan ook. In kleinere organisaties doen we ze allemaal in één keer en soms heb je ook dat je eerst het management en dan het verpleegkundig personeel doet. Het is dus heel afhankelijk van de wensen van de organisatie en de organisatiestructuur.

RS: Ja, en maak je dan ook onderscheid in de manier waarop je die groepen benadert of krijgen ze allemaal dezelfde training?

IO: Daar maken we wel onderscheid in. Het is altijd een training op maat het is nooit hetzelfde, want de ene organisatie is de andere niet en je kunt het soms net iets anders uit de praktijk benaderen. Het is altijd maatwerk.

MVD: En daaraan voorafgaand houden we vaak ook eerst een enquête om informatie naar boven te krijgen en die verwerken we dan in de training, zodat je ook de training levendig kunt houden voor de medewerker en ze hun eigen praktijkvoorbeelden daarin kunnen herkennen. Inderdaad een training bij een ICT-leverancier is niet hetzelfde als een training bij een zorginstelling.

RS: Nee, nee zeker niet natuurlijk. Wat voor enquête is dat dan? Wat voor soort vragen worden daarin gesteld?

IO: Vragen waarmee we toetsen hoe bewust medewerkers al zijn en dan kunnen dat weer hele verschillende vragen zijn. Voorbeelden daarvan zijn: Ben je je bewust van het doel dat er binnen de organisatie geldt? Is dit doel in overeenstemming met de wijze waarop je de gegevens verwerkt. Het zijn vragen die je met ja of nee kunt beantwoorden en dan volgt daar een score uit. Je merkt uit de uitslagen van de enquêtes dat medewerkers wel enigszins bewust zijn hoor, maar je merkt ook wel dat heel veel onbewust onbekwaam is en wat wij dan eigenlijk doen is er in ieder geval voor zorgen dat ze bewust bekwaam worden.

RS: Ja, dat is natuurlijk het beste.

MVD: Als mensen zich realiseren 'oh er speelt veel meer dan dat ik dacht, oh heeft dit er ook mee te maken' dan is stap 1 al gezet.

RS: Ja, dat is natuurlijk een goede stap. Daar zijn die trainingen ook handig voor. Zijn er nog andere manieren waarop je probeert de mensen in de organisatie mee te krijgen?

IO: Ja, we hangen wel eens quotes op of uitleg over bepaalde onderwerpen en we sturen deze informatie rond, maar we gebruiken met name de trainingen. De mensen krijgen we met de trainingen over het algemeen wel mee.

RS: Want merk je nu ook bijvoorbeeld verschillen nu de Meldplicht Datalekken is ingegaan 1 januari in de bewustwording van de organisatie?

IO: Ja, organisaties weten dat het er is en zijn zich ervan bewust dat ze er iets mee moeten.
MVD: Ja, je merkt wel dat het bewustzijn blijft hangen bij de zoekgeraakte usb-stick. Dus de hele nadrukkelijke voorbeelden, maar de voorbeelden als 'oh oeps sorry ik heb per ongeluk een verkeerd e-mailadres gebruikt of deze persoon had deze gegevens überhaupt helemaal niet mogen inzien en die kan er altijd al bij', daar staat men dan niet bij stil dat dit ook datalekken zijn.

RS: Ja, ik kan me ook voorstellen dat de drempel best hoog is voor medewerkers om dat soort dingen te melden, terwijl iets als een verloren usb-stick of een laptop dat is toch iets wat een beetje buiten jouw eigen…

MVD: Precies. Het is een drempel, maar men heeft vooral ook niet door dat dat ook niet mag.

RS: Oké dat is wel interessant, dat men dat niet doorheeft. En in hoeverre denken jullie dan dat communicatie een rol zou kunnen spelen in het inperken van de risico's op een datalek?

MVD: Ik denk dat het een belangrijk onderdeel is. Wat ik net al zei, op het moment dat je het in de communicatie goed oppakt, kun je het klein houden. In trainingen brengen we ook wel eens dat voorbeeld naar voren van de gemeente Amersfoort. De medewerker heeft het niet gemeld, die heeft het onder de pet gehouden. Vervolgens is het wel gemeld, maar is er ook in de communicatie niet goed mee omgegaan. Vervolgens heeft dat weken lang in de media en social media door geëtterd. Terwijl als het gewoon goed gemeld was en vervolgens goed opgepakt, dan was het helemaal niet zo'n big issue geweest denk ik.

RS: Nee, nou zie je natuurlijk in de media dat het volgens mij sinds een paar maanden een enorm ding is. Dus je ziet alle datalekken terugkomen, ook die in de zorg. Bijvoorbeeld het Antoni van Leeuwenziekenhuis had er

één. Dus dat kan natuurlijk ook bijdragen aan dat mensen er meer mee bezig gaan. En als je dan een privacybeleid zou instellen voor zorginstellingen wat zou dan idealiter geregeld moeten zijn?

IO: Heel veel.

MVD: Dat is een hele brede vraag inderdaad.

RS: En bijvoorbeeld op verschillende niveaus op het niveau van beleid of medewerkers.

IO: Ja, eigenlijk alles, je probeert alles wel mee te nemen. Ik zal je een beetje meenemen in onze aanpak: wat wij doen is eigenlijk wij kijken naar de dingen als een privacystatement is dat er op de website? Cookiebeleid is daar over nagedacht? Welke bewerkingen vinden er binnen de organisatie plaats? Dan maken we daar een register van, wat ook straks voor de Europese Verordening verplicht is. Dan bouwen we eigenlijk een soort van beleid aan de hand van kleine stukjes. Op het moment dat we dat bij elkaar gooien dan vormt het zich vanzelf een beetje en dan kun je ook naar een beleid toewerken dat door de hele organisatie gedragen wordt en dat is een beleid wat op alle niveaus werkt. Van de receptie tot aan de bestuurder.

RS: Dus dan maken jullie eigenlijk die QuickScan waar jullie het over hadden die maken jullie eigenlijk voor elke organisatie?

MVD: Ja, feitelijk moet je de hele organisatie in kaart brengen wil je je beleid goed op orde hebben. Dus we beginnen er niet mee bij elke organisatie, maar op een gegeven moment, werken we ook al toe naar de verplichting die de Europese Verordening strakjes stelt. Bijvoorbeeld het hebben van een register van verwerkingen, dat is een heel ander onderwerp dan datalekken natuurlijk, maar als je je register op wil stellen dan moet je ook al je organisatie in kaart hebben, dus dan helpt zo'n QuickScan ook al om daar de basis voor te leggen. Dan heb je in ieder geval je verwerkingen in kaart en kun je vervolgens vragen behandelen als: Welke type persoonsgegevens verwerken we? Wie mag erbij? Voor wat voor doel worden zaken bewaard of verwerkt? Dus die QuickScan, ja wij noemen het QuickScan maar eigenlijk moet je de vervolgstap ook doen: De Privacy Impact Assessment. De QuickScan is daar de eerste stap in, de basis eigenlijk. Wij noemen het ook wel nulmeting.

RS: Ja, want dan kun je natuurlijk ook gericht aan de organisatie koppelen.

IO: Ja, het is een nulmeting eigenlijk hè. Die voeren we uit om even de status quo te weten en te weten waar staat de organisatie staat. Bij organisaties die nog niks geregeld hebben doen we bijvoorbeeld geen Quickscan. Dat is ook niet nodig. Maar bijvoorbeeld zo'n PIA (Privacy Impact Assessment), dat is straks verplichten dat is iets wat we licht doen in de privacy-QuickScan omdat de vragen die we stellen deels overeenkomen. Veel beter is het om de PIA's te doen, omdat deze analyse veel completer is en uitgebreider. We toetsen dan de verschillende diensten.

RS: Ja, want het is nu natuurlijk een soort tussenperiode. Je hebt nu wel de Meldplicht Datalekken en de Europese Verordening bestaat ook al, maar treedt pas in werking in 2018. In hoeverre denken jullie dat zorginstellingen daarop voorbereid zijn in mei 2018?

MVD: Ja, nou daar werken wij nu hard aan om daarvoor te zorgen dat zorginstellingen inderdaad daar klaar voor zijn, want nu heb je nog bijna anderhalf jaar de tijd. Langzamerhand begint het kwartje een beetje te vallen, de bewustwording wordt steeds groter. Wij zijn er nu driekwartjaar aan het trekken om dat op de agenda te krijgen en je merkt nu eigenlijk de laatste maanden dat het steeds hoger op de agenda komt te staan.

RS: Ja, want hoe komen jullie in contact met de zorginstellingen waarvoor jullie werken? Zijn er bijvoorbeeld evenementen of iets dergelijks? Of hoe komen die mensen bij jullie? Want dat is natuurlijk ook al een stap die die mensen zetten van we hebben iemand nodig hiervoor.

IO: Ja, we zijn natuurlijk een bedrijf dat uiteenlopende consultancydiensten aanbiedt aan de zorgsector. We hebben dus ook consultants met klanten die zij bij ons kunnen aandragen omdat ze op zoek zijn naar ondersteuning op het gebied van privacy. Dus we hebben met elkaar al een groot netwerk, omdat we binnen Cure4 aanvullende dienstverleningen hebben voor de zorgsector. Daarnaast hebben we onze salesmanager die nieuwe en bestaande klanten met een aanvullende vraag aanbrengt. Die is daar erg goed in, het aantrekken van nieuwe contacten en het onderhouden van bestaande. Bovendien bezoeken wij ook regelmatig evenementen waar we zorginstellingen tegenkomen en bloggen over verschillende onderwerpen waardoor klanten ook bij ons terecht komen.

MVD: We publiceren zaken ook bijvoorbeeld op LinkedIn en daar krijgen we ook reacties op. Wij proberen gewoon heel erg veel kennis te delen en daarmee ook eigenlijk organisaties bewust te maken van wat er allemaal speelt. En daar zie je ook reacties op van: 'hee oké ik moet dit geregeld hebben, ik moet hier iets mee'.

RS: Ja, want zijn organisaties zelf dan nog heel erg bezig met die Meldplicht Datalekken of zijn ze ook echt al over de Europese Verordening aan het nadenken?

MVD: Nee, over de verordening zijn ze nog helemaal niet aan het nadenken. Het is met name dat we merken dat zorginstellingen doorhebben dat ze iets moeten met privacy, maar ze hebben geen idee wat eigenlijk. Bijvoorbeeld: "Ik moet bewerkersovereenkomsten hebben maar hoe doe ik dat dan?"

RS: Dus eigenlijk er is wel een soort bewustzijn van ik moet iets met privacy en de bescherming van persoonsgegevens.

MVD: En sommige organisaties hebben dat wat scherper op het netvlies dan andere.

IO: Dat is letterlijk wat we vaker horen. We moeten iets met privacy maar we weten niet wat.

RS: En wat zijn dan lastige punten om zo'n beleid door te voeren of in ieder geval onder de aandacht te brengen. Ik kan me voorstellen dat ze soms ook geen budget hebben, geen zin hebben om mee bezig te gaan.

MVD: Ja, het budget is een ding, maar op het moment dat je het projectmatig uitsmeert over de tijd kan dit meevallen. Daarom hameren we er nu ook zo erg op dat zorginstellingen nu nog anderhalf jaar hebben. Je hoeft het niet nu in een keer voor 1 januari geregeld te hebben, neem nou die tijd en dan kunnen we dat punt over het algemeen nog wel tackelen. Maar wat je ook ziet is dat organisaties aangeven: medewerkers moeten al zoveel. Ze moeten al zoveel trainingen volgen, ze moeten al aan zoveel kwaliteitseisen voldoen en dan komt dit daar ook nog bij. Dus het wordt ervaren als nog weer een extra druk op de organisatie en dat schuiven ze het liefst zo ver mogelijk voor zich uit.

IO: Het is nog geen onderdeel van het geheel. Dus dat merk je wel heel erg. Die transitiefase daar zitten we middenin. Privacy moet echt nog een onderdeel worden van de organisaties, maar ook bijvoorbeeld een onderdeel vormen van de kwaliteit en certificeringen binnen de organisatie. Het is het allermoeilijkst om daar naartoe te werken, zodat het een onderdeel is van het grote geheel. Ik denk dat dit tijd nodig heeft en dat het over een paar jaar wel los loopt.

MVD: Ja, het moet onderdeel worden van het hele kwaliteitssysteem, onderdeel van goede zorg.

RS: Het is natuurlijk ook een lastige groep, zeker in GGZ-instellingen ook. Er is natuurlijk heel veel reorganisatie in de zorg dus dat kan meespelen, maar hoe kijken bestuurders daar tegenaan dan? Zien zij hier de prioriteit van in? Of hebben ze ook nog een ander lijstje liggen wat ze eerst geregeld willen hebben?

IO: Ja, dat laatste inderdaad.

RS: En hoe zorgen jullie dan dat ze wel met privacy beziggaan?

MVD: Nou, we proberen het met name zo laagdrempelig mogelijk te houden door inderdaad te ontzorgen. En we pakken het projectmatig aan op basis van prioriteiten, die wij samen opstellen. Dus bijvoorbeeld je hebt nu weinig ruimte tot 1 januari, het is nu half november laten we dan tot 1 januari in ieder geval dit project oppakken en vervolgens maken we een plan voor een bepaalde periode waarin we in overleg proberen dat te doen en zo min mogelijk druk bij de organisatie leggen.

RS: Ja en wat zijn dan meestal de eerste prioriteitspunten voor zo'n organisatie?

MVD: Medewerkers bewust maken toch, toch een training. En wat men wel heel belangrijk vindt is het organiseren van toeleveranciers, de bewerkers. Maar ook de overeenkomst van dienstverlening met zo'n leverancier Dat hangt natuurlijk samen met de bewerkersovereenkomst. Dus eigenlijk het grip krijgen op je leveranciers en dat is dan weer gekoppeld aan datalekken. Op het moment dat je zegt er gaat iets bij je leverancier mis hoe ga je dat managen? Dat kan volgende week zomaar ineens gebeuren, dan merk je dat dat ineens wel naar voren komt.

RS: Ja, want zijn er ook al meldingen binnengekomen bij de zorginstellingen waar jullie werken?

IO: Meldingen van datalekken bedoel je? Ja, die vinden wel plaats.

RS: En komen die dan meestal vanuit medewerkers of komen die van mensen hoger in de organisatie?

MVD: Meestal wel van onderaf. Medewerkers zien dingen gebeuren.

RS: Ja, dus die melden dat dan bijvoorbeeld bij hun leidinggevende. En zijn er ook al meldingen gedaan bij de Autoriteit Persoonsgegevens?

IO: Wel door de zorginstellingen, nog niet door ons persoonlijk.

RS: Want hoe kijken jullie tegen die rol aan van Autoriteit?

IO: Hoe bedoel je dat?

RS: Als in hoe zien jullie hen?

IO: Als autoriteit? Zij willen graag een rol daarin spelen en er is helaas nog geen boete uitgedeeld, dus dat mis ik wel een beetje. Dat moet er eigenlijk wel komen om het op gang te helpen, zodat je ook het proces een beetje kan versnellen en je organisaties wat meer compliant kunt maken voordat die Europese Verordening dadelijk in werking is getreden. Maar ja hoe kijken we daar verder naar? Het is een prima auoriteit. Hun website is bijvoorbeeld heel goed en informatief met veel uitleg en geeft veel houvast. Dus dat is denk ik een beetje hoe we er tegenaan kijken.

RS: Ja, want hebben ze ook bijvoorbeeld informatie gestuurd naar zorginstellingen waarvoor jullie werken?

MVD: Ja ze hebben algemene brieven gestuurd aan de Raden van Bestuur aan het begin van dit jaar waarin ze aangeven, dat bepaalde zaken niet op orde zijn, maar dat is niet gericht aan de opdrachtgevers van ons. Dat zijn algemene brieven geweest die ze verstuurd hebben.

RS: Ja, ze hebben natuurlijk ook vrij weinig capaciteit.

MVD: Ja precies dat is het punt. Je meldt een datalek, maar je hoort er uiteindelijk nooit meer iets van terug. Dus dat is ook wel de kritiek. Ze geven wel adviezen en als ze onderzoek doen dan publiceren ze dat ook wel, maar als je het hebt over het wel of niet melden en dat er geen boetes uitgedeeld worden. Dat helpt niet om dit in beleid op een goede manier van de grond te krijgen. Het mag wat concreter worden.

RS: De wet zelf is op sommige vlakken ook wat onduidelijk volgens mij. Ik was bij een bijeenkomst geweest van de NVFG (Nederlands Vakgenootschap voor Functionarissen van de Gegevensbescherming) Daar was ook iemand van de Autoriteit Persoonsgegevens aanwezig, Udo Oelen heette hij geloof ik en die beantwoordde vragen, maar er waren volgens mij nog wel wat onduidelijkheden in de wet.

MVD: Ja er zijn een heleboel open normen en die moeten ingevuld worden. Maar aan de andere kant ik zie dat niet direct als een nadeel. Mijn mening is wel dat op het moment dat je een open norm hebt dan moet je die vertalen naar een organisatie en als je daarover nadenkt en onderbouwt waarom je welke keuzes maakt, dan maak je op die manier een passende invulling van die norm. Dus het geeft je ook wel flexibiliteit.

IO: Bovendien kan de techniek ook meebewegen en dat is vooral heel erg belangrijk. Dus ik denk dat die open normen ook wel een functie hebben, anders moet je elke keer wetswijzigingen doorvoeren om bij te blijven. Dus wat is inderdaad een goede technische maatregel en wanneer ben je compliant en heb je de juiste technische maatregelen getroffen. Ja, dat kan heel erg wisselend zijn per bedrijf en per geval. Dat moet je in de context bekijken en dat is dus lastig.

MVD: Ja, dat is zo. Maar beleidsmatig is het dan wel van belang dat je het gewoon goed onderbouwt. De stappen die je zet, de keuzes die je maakt, beargumenteer die en als dan achteraf blijkt dat het anders is dan kun je in ieder geval al wel laten zien dat je erover nagedacht hebt en dat je niet over één nacht ijs gegaan bent met deze keuze en dat geeft je ook de mogelijkheid om bij te sturen. Dan kun je het wel elke keer beredeneerd doen.

RS: Ja, ik kan me aan de andere kant ook wel voorstellen dat ze nog geen boetes hebben gegeven, want het kan natuurlijk ook averechts werken, dat mensen denken dat als er boetes opgelegd worden, we gaan het dus niet melden.

IO: Ja, maar op het niet melden staat een boete.

RS: Ja, klopt

MVD: En als je een datalek hebt en je meldt het dan krijg je op grond daarvan in elk geval geen boete. Maar op het moment dat jij je organisatie op orde hebt, je hebt voldoende maatregelen genomen, je beleid is op orde, je medewerkers zijn getraind en je krijgt een datalek. Als je dan een onderzoek zou krijgen en je kunt dat hele verhaal gewoon goed onderbouwen, dan zul je ook niet zo snel een boete krijgen. Je zult dan hooguit een aanwijzing krijgen om op een bepaald punt bijvoorbeeld bij te sturen.

RS: Ja, maar dat is dan wel een beetje een ideale situatie natuurlijk dat een bedrijf dat allemaal op orde heeft, wat nu waarschijnlijk nog niet het geval is.

MVD: Nee, precies, maar daarom is het dus zo belangrijk om die processen op orde te gaan krijgen. En als straks die verordening in werking treedt en je hebt een datalek en je meldt dat omdat het ook al een journalist heeft gevonden, kun je het niet meer onder de pet houden. Als dan blijkt dat jij deze periode niet de moeite hebt genomen je organisatie op orde te brengen, ja dan ben je wel redelijk nalatig geweest.

RS: Ja, en hoe is die procedure omtrent datalekken dan ingericht voor de zorginstellingen? Hebben jullie daar een bepaalde procedure voor die jullie overhandigen of verschilt dat heel erg?

IO: Ja het is een stappenplan eigenlijk met een aantal stappen die dan doorlopen moeten worden, waarmee dan alle informatie verzameld wordt die nodig is om te loggen of om een melding te doen.

RS: Ja en zijn jullie dan degene die dan uiteindelijk melden bij de Autoriteit Persoonsgegevens of is dat dan iemand van de organisatie?

IO: Ja, dat kan allebei. Dus afhankelijk van de situatie.

RS: Oké en is dat stappenplan een beetje vergelijkbaar met wat op de site van de Autoriteit Persoonsgegevens staat?

MVD: Daar staat alle informatie die je aan moet leveren en het stappenplan dat wij ontwikkeld hebben dat heeft eigenlijk een vertaling gemaakt van die informatie van de autoriteit. Wie moet wanneer waarbij betrokken worden. Ook de onderliggende bewerkers komen in een stap naar voren zodat je snel boven water hebt waar je informatie vandaan moet halen om vervolgens weer de vervolgstap op de site van de autoriteit te kunnen invullen.

RS: Ja, want beschikken de zorginstellingen bijvoorbeeld over een intern meldpunt?

IO: Ja, dat is ook weer afhankelijk van de instelling. Als het een kleine is, ja dan is er niet echt een centraal punt of iets dergelijks. Maar als het een grote is dan is er heel veel al wel op orde en dan kan het daarop aansluiten omdat er ook voor andere incidenten bijvoorbeeld een meldingsprocedure is.

MVD: Sluit vaak aan bij de kwaliteitsmeldingen, daar is vaak al wel een meldpunt voor.

RS: Ja.

MVD: als je hem daarbij aan laat sluiten dan is het ook niet een extra belasting, maar sluit het gewoon aan bij het kwaliteitssysteem.

RS: Ja, dat zie je vaker gebeuren inderdaad dat ze een bepaald kopje ervoor maken en dat je dan op die manier kunt melden. Even kijken want volgens mij heb ik zo'n beetje alles gevraagd wat ik wilde vragen. Even kijken of ik nog niet iets belangrijks vergeet. Oja, nog wel een leuke misschien: wat zou mensen gaan motiveren om te gaan melden binnen de instellingen.

IO: Ik denk dat het uitdelen van boetes daar een rol in kan spelen. Dit is wellicht een verkeerde methode, want men zou moeten melden zonder dat er een boete dreigt, maar dit is en blijft lastig.

MVD: wat zou mensen motiveren om te gaan melden? Nou ja kijk dat is wel een beetje vanuit een negatieve invalshoek, medewerkers willen niet op hun geweten hebben dat het misgaat en zij de oorzaak zijn, maar dat is een negatieve invalshoek. Je ziet wel dat mensen in een vorm van paniekreactie zeggen: 'oh oeps dit moet ik wel gaan melden', maar ja dat is niet echt motivatie, maar dat is meer dat ze de schade voor zichzelf willen beperken.

RS: Ja, want zien jullie nu ook meer meldingen binnenkomen in de loop van het jaar? Dat medewerkers vaker met incidenten komen of met vragen?

MVD: Met vragen dat is het meer, het is niet zozeer het melden van incidenten maar wel met vragen van hoe kan ik hiermee omgaan. Dat merk je wel meer.

RS: En er is de afgelopen tijd de 'ZEKER' campagne geweest van de NVZ. Hebben de instellingen waarmee jullie werken hier ook aan mee gedaan?

IO: We hebben wel een geleide ontvanger daarvan, maar in hoeverre de instellingen daaraan mee hebben gedaan dan moet ik je eerlijk zeggen dat ik je dat antwoord schuldig moet blijven.

RS: Ja, want ik vroeg me dat inderdaad af, want ik zag dat 80 zorginstellingen eraan mee gedaan hebben. Je kan je afvragen wat voor zorginstellingen dat waren. Ze hadden bijvoorbeeld ook een quiz voor medewerkers om die bewust te maken. Ik weet niet of jullie bekend zijn met die campagne. Daar kwam dus uit dat medewerkers goed voorbereid zijn en zich heel erg bewust zijn van privacy, dus daar zette ik meteen mijn vraagtekens bij. Ik ben dit nog niet echt tegengekomen in de praktijk, hoe zit dit?

IO: Ja, wij hebben toevallig zelf een benchmark laten doen in het voorjaar was dat, maar daar kwam juist uit dat zorginstellingen een lage awareness hebben op het gebied van privacy. Dus het zal misschien ook aan de vraagstelling hebben gelegen.

MVD: Ja, heb je de vragen gezien?

RS: Ja, ik heb de quiz gedaan en gedaan of ik van een zorginstelling was, maar dan krijg je inderdaad vragen als, hij staat nog wel online dus je kunt hem nog wel vinden, medewerker gaat koffie halen of iets dergelijks en vergeet zijn pc uit te loggen, wat doe je? Het maakt ze natuurlijk wel bewust, maar de uitslagen zijn niet representatief.

MVD: Ja, als je dan de conclusie trekt dat mensen aware zijn, dan klopt dat niet helemaal.

RS: Ja, dat zijn dan van die dingen daar kijken wij vanuit communicatie natuurlijk heel erg naar als we een enquête opstellen. De vraagstelling is super belangrijk hoe je iets aan iemand vraagt. Ik was wel benieuwd of jullie er bekend mee waren en of instellingen er aan mee hebben gedaan.

IO: Ik heb het niet gehoord, ik heb wel gehoord dat het leefde bij verschillende instellingen. Ik denk dat ze er wel aan meegedaan hebben sommigen.

MVD: De vraag is ook natuurlijk welke medewerkers hebben het dan ingevuld, was dat zichtbaar in de data?

RS: Nou het was echt een heel kort nieuwsbericht, in ieder geval een heleboel.

MVD: Vult de security officer dat in of de verpleegkundige dat maakt nogal wat uit denk ik.

RS: Het was door 2000 medewerkers ingevuld, dus het zijn er wel best wat. Maar per zorginstelling zijn er vaak al wel 2000 medewerkers. Het zijn natuurlijk wel stappen die je hierin moet nemen, want bijvoorbeeld ook in mijn onderzoek kan ik geen enquête uitsturen naar alle zorginstellingen in Nederland wat ze allemaal aan communicatie doen op dit vlak, want dat zal er in veel gevallen misschien nog wel niet zijn. Ook wel berichten hierover teruggekregen dat het nog niet aanwezig is bij sommige instellingen.

Nagesprek, bedankt voor het interview.

Bijlage 4.2 Interview Awareways

Integrale programma Awareways

GV: 'Het eerste wat we altijd doen is de mate van volwassenheid binnen een organisatie meten. Dat doen we op zes variabelen van gedrag. Daarvoor gebruiken we de Theory of Planned Behaviour. Dat is een theorie uit de psychologie. We meten de norm binnen de organisatie, we meten wat de houding is en een houding die kun je weer onderverdelen in: is het beschikbaar, is het relevant en is er interesse. Dan meten we het kenniscomponent. We meten de controle die mensen ervaren en het uiteindelijke gedrag. En op al die facetten scoren we een organisatie en dan zien we waar een organisatie slecht op scoort.

Het is een vragenlijst van 55 vragen die wij samen hebben ontwikkeld met de Universiteit Utrecht. Het komt veel voor dat organisaties slecht scoren op de norm. Het is bijvoorbeeld niet de cultuur van een organisatie om een computer te locken of iemand erop aan te spreken als die het niet goed doet. Dat gaat om normenpatronen en culturele waarden die in een organisatie omhoog moeten, maar we zien ook problemen in de kennis. Mensen weten bijvoorbeeld niet hoe ze phishingmails moeten herkennen of mensen weten niet wanneer een wachtwoord veilig is. Dus dat zijn van die kleine dingen die je mensen kunt leren: praktische kennis. En op de norm kun je met behulp van campagnevoering heel goed invloed uitoefenen. Dus aan al die knoppen kunnen we draaien.

Op het moment dat we een heel goed beeld hebben van een organisatie, ontwikkelen we een programma. Dat programma bestaat uit verschillende bouwstenen. Eén daarvan is e-learning. Wij doen toch nog vrij veel wel met sessies. Ambassadeurssessies maar ook managementsessies om mensen ook verantwoordelijk te maken binnen een organisatie. Wij noemen dat ook wel de BHV'er van de

informatiebeveiliging. We doen ook wel aan red teaming. Dan kijken we hoe makkelijk we ergens binnenkomen en confronteren we daar vervolgens de board mee'.

GV: 'We hebben inmiddels 10 modules in allerlei talen waaronder social engineering, phishing, flexibel werken, passwords en veilig omgaan met mobile devices. We hebben een scenario ontwikkeld van een willekeurige werkdag uit het leven van onze actrice: in wat voor situaties kom je terecht waar mogelijke risico's zich voordoen? Van ik stap in de trein, naar ik ben op mijn werk, naar ik heb een afspraak buiten de deur, naar ik ga weer terug naar huis. Wat kom je dan tegen?'

GV: 'Organisaties maken zelf een keuze op basis van de issues die spelen. De meting geeft ook inzicht in de issues die bij een organisatie spelen, zoals de antwoorden van medewerkers op vragen over wachtwoorden en computers locken'.

GV: 'Wat we heel veel doen is ambassadeurssessies. Zo'n sessie bestaat uit inspireren, interesseren en shockeren. Dus dan heb je mensen geprimed en dan zijn mensen positiever voordat ze zo'n e-learning gaan doen omdat we hun houding al beïnvloed hebben'.

Ook doet Awareways personeelsbijeenkomsten waar ook criticasters bij zijn. Zij zijn kritisch en hebben daar een reden voor, dus dan gaat Awareways opzoek naar hun weerstanden. Daarnaast ontwikkelt Veenbergen ook trendsessies waarbij op board en c-level organisaties geïnspireerd worden door hen te laten zien waar we over tien jaar staan en wat dat betekent voor je medewerkers, voor security awareness en voor je technische beveiliging. Dit helpt organisaties verder te kijken dan alleen nu brandjes te blussen.

Het programma duurt sowieso een jaar, omdat je verschillende e-learningmodules hebt. De periode waarin het programma wordt ingezet is afhankelijk van hoeveel een organisatie wil doen, maar je bent al gauw een jaar onderweg met elkaar. E-learningmodules worden afgewisseld met sessies en er worden bijvoorbeeld ook phishingmails verstuurd, waarbij uitleg verschijnt voor medewerkers dat ze op een phishingmail hebben geklikt of een lifehackingsessie georganiseerd.

Samenwerking met organisaties

GV: 'Ik werk heel nauw samen met communicatie en HR om ervoor te zorgen dat informatiebeveiliging en informatiebewustzijn een topic blijft in de organisatie. We proberen vaak ook ons programma binnen organisaties in de HR-cyclus te krijgen zodat het ook echt onderdeel wordt van het functioneren van iemand. Bij verzekeraars en banken gaat dat ontzettend goed, maar bij een NGO bijvoorbeeld vinden ze dat heel spannend. Met de communicatieafdeling kijken we hoe het onderwerp ingebouwd kan worden in de jaarlijkse interne communicatiekalender. Dat zijn de basiselementen die we implementeren en integreren en vervolgens is het bijsturen. Uit die modules komt allerlei rapportage en dan zie je bijvoorbeeld: ze scoren slecht op phishing dus daar moeten we extra aandacht aan besteden'.

Veenbergen geeft aan dat de ingang in de organisatie vaak via IT is of via de board. 'Wij vragen dan vaak of we om tafel kunnen met IT, communicatie, HR en iemand van de board, omdat dit belangrijke mensen zijn om te betrekken in dit verhaal. Beveiliging is de verantwoordelijkheid van de hele organisatie en niet alleen van IT. Kijk uiteindelijk heb je allemaal dezelfde verantwoordelijkheid binnen een organisatie en dat is zorgen dat de continuïteit van de organisatie door kan gaan. En HR heeft daar een andere functie in dan IT, maar je hebt wel dezelfde doelstelling. Je moet opzoek gaan naar de overkoepelende doelstelling en vragen wat ieders verantwoordelijkheid daarin is. Dus wij zijn er ook om begrip te krijgen tussen de afdelingen en aan te geven dat je zonder optimale beveiliging niet verder kan.

Awareness is al langer belangrijk thema

Veenbergen geeft aan dat er in 2000 ook al wel aandacht aan awareness werd gegeven op dit gebied door bijvoorbeeld SANS. SANS is een internationaal opererende partij die de levels van maturity op security awareness heeft ontwikkeld en ook door mensen als Edward Snowden is er al eerder aandacht aan gegeven. Door de aangescherpte wet- en regelgeving merk je wel dat het ineens hard gaat. Ook zijn er nieuwe trends en ontwikkelingen zoals the Internet of Things, mensen die met hun eigen devices werken, auto's die verbonden zijn met het internet. Dit zorgt wel voor een mind change.

Evaluatie van programma
GV: 'De meting, de phishingsoftware en de e-learning zijn allemaal meetbaar. En campagnes die zijn afhankelijk van of het een kwalitatieve of kwantitatieve campagne is ook meetbaar. Binnen onze meting zit ook de Netto Promotor Score. Dus op allerlei vlakken komt er een rapportage uit van hoe effectief een organisatie is en dan doen we aan het einde van het traject een éénmeting'.

Awareness is een doorlopend onderwerp
GV: 'Awareness is een doorlopend onderwerp en daarom proberen we het ook binnen communicatie op de agenda te krijgen als onderwerp. Uiteindelijk is een organisatie natuurlijk zelf verantwoordelijk om de beveiliging op niveau te houden en daar hoort awareness ook bij. Dus je kunt ervoor kiezen om sessies te blijven herhalen'.

Niet genoeg tijd investeren in goed beveiligde software
Awareways werkt veel met een ethical hacker samen en die geeft aan dat alle software die we nu hebben gemaakt worden om een bepaalde functie daaraan toe te kennen, maar daarbij wordt niet gedacht aan de beveiliging. Dus alle software die we nu gebruiken die is hartstikke lek, omdat we niet genoeg tijd investeren in goed beveiligde software. GV: 'Wij zitten heel erg op de eindgebruiker, maar we moeten ook nadenken over makers'.

Bijlage 4.3 Interview Duthler Academy

Samenvatting Interview Anneke van der Heijden - Programma Awareness Raising Duthler Academy & Leergang FG

Duthler Academy ondersteunt bedrijven en instellingen bij het organiseren van kennis en ervaring op het gebied van gegevensbescherming en privacy. Het is een volledige dienstverlening gericht op het ontzorgen van leiding. Voor alle medewerkers, van schoonmaker tot directeur, is passende opleiding beschikbaar.

Van der Heijden verzorgt het awareness raising programma bij Duthler Academy. Duthler Academy heeft daarnaast een leergang FG. Deze opleiding bestaat uit 30 modules, die worden gemaakt door Duthler terwijl de opleiding bezig is. Van der Heijden zit in de eerste lichting van deze opleiding. Van der Heijden: 'De modules worden continu aangepast en vernieuwd aan de veranderende wetgeving, want er veranderen ook altijd dingen in de praktijk. Je kunt kiezen voor een complete opleiding of voor een aantal modules. Je hebt ook stepup cursussen voor managers en raden van bestuur. Deze stepup cursussen praten managers in drie dagen bij in 6 modules. Hier horen ook tentamens bij en als ze willen kunnen ze ook meer modules volgen'.

Het programma wordt gekenmerkt door herhaling en dat het een langdurig programma is.

'Je ziet nu vaak dat privacy iets voor de ICT is en voor mensen met een juridische achtergrond, maar het is eigenlijk een organisatievraagstuk' Van der Heijden geeft aan dat juristen vaak vanuit hun werk ervaring hebben met privacywetgeving, maar niet met de nieuwe wetgeving. Het is daarom veel te veel om te weten voor juristen, ze weten lang niet alles. Het is bijvoorbeeld ook interessant om te kijken wie in de organisatie zorgen voor datalekken, dan blijkt dit in 19% van de gevallen ICT-personeel te zijn, dus zelfs daar ontbreekt het bewustzijn. Van der Heijden geeft aan dat functionarissen gegevensbescherming op dit moment vaak onvoldoende kennis hebben om hun functie goed te vervullen. En zeker omdat een FG in een organisatie een beschermde titel heeft, is het van belang dat hier iemand zit met verstand van zaken.

Van der Heijden geeft aan dat privacy meer een organisatievraagstuk is en daaromheen heeft ze het programma awareness raising opgezet. Van der Heijden geeft aan: 'Iedereen in de organisatie moet dit volgen, niet alleen ICT-mensen, maar het is voor iedereen van belang'. Het Programma Awareness Raising bestaat onder andere uit een e-learning. Deze training kent drie niveaus:

-Het basisniveau. Hierin wordt besproken wat privacy is, waar het vandaan komt en wat de wetgeving inhoudt. Deze training is geschikt voor iedereen in de organisatie.

-Het tweede niveau. Deze training wordt gevolgd door mensen die veel doen met persoonsgegevens, maar niet met bijzondere persoonsgegevens.

-Het derde niveau: Dit niveau wordt gevolgd door leidinggevenden en mensen die werken met

Van der Heijden laat zien hoe de e-learningmodule eruit ziet en geeft aan dat er steeds één onderwerp wordt besproken. Er wordt besproken wat de risico's zijn en hoe deze vermeden kunnen worden. De modules bestaan uit korte filmpjes en animaties, die worden afgewisseld met interactieve vragen en spelletjes. De onderwerpen die besproken worden zijn: introductie en doel, beveiliging, persoonsgegevens, werkplek en omgeving, datalek en veilig internetgebruik. Om de module af te ronden, moet je een test doen en de uitkomsten van deze test zijn bepalend voor of je door mag naar de volgende module.

Bijlage 5 Uitwerkingen interviews zorginstellingen

5.1 Uitwerking Interview zorginstelling A

RS: De functie van privacy officer is natuurlijk vrij nieuw. Hoe ben je precies bij deze functie terechtgekomen?

Zorginstelling A: Oh uhm, nou ik ben twee jaar geleden begonnen bij zorginstelling A ik heb daar ook mijn afstudeeronderzoek gedaan. En toen is de zorginstelling begonnen met een impact en risicoanalyse in het kader van privacy omdat de Algemene Verordening Gegevensbescherming (in het vervolg afgekort tot AVG) er aan zat te komen vanuit Europa die nu van kracht is hè vanaf mei. En op dat moment ben ik eigenlijk begonnen als jurist in het project dat die analyse ging doen en op dat moment was er al een functionaris gegevensbescherming (in het vervolg afgekort tot FG) werkzaam parttime. Toen bleek uit de analyse dat er toch wel wat werk aan de winkel was om te gaan voldoen aan de nieuwe AVG en toen hebben ze mij gevraagd eigenlijk of ik ook die functie wilde gaan doen, dus eigenlijk zodoende, omdat er gewoon de noodzaak was. Er moet wat gebeuren: de 24-uurscapaciteit die er was, was toch wel wat weinig, dus ben ik er bijgekomen voor 24 uur. Dus 48 uur FG.

RS: Ja, dus daarnaast ben je nog gewoon jurist?

Zorginstelling A: Nee, ik ben alleen FG wel met een juridische achtergrond natuurlijk en mijn collega had dat niet, dus dat was ook wel een pré dat ze mij graag wilden.

RS: Het is natuurlijk met dat soort dingen altijd een beetje kijken, privacy officer is een redelijk nieuw iets dat iedereen het moet hebben, dus daarom ook deze vraag, zodat we een beetje in kaart kunnen brengen wat iedereen voor achtergrond heeft.

Zorginstelling A: Het is wel functionaris voor de gegevensbescherming dat is een wettelijk vastgelegde functie. Privacy Officer is dat niet.

RS: Oké daar zit wel een verschil tussen?

Zorginstelling A: Ik heb zeg maar ontslagbescherming en ik moet onafhankelijk zijn en bepaalde taken zijn ook wettelijk vastgelegd zoals toezicht houden. Privacy officer is dat officieel niet.

RS: Oké dus er zit wel daadwerkelijk verschil tussen, want inderdaad daar was ik ook benieuwd naar: je hebt natuurlijk privacy en je hebt bescherming van persoonsgegevens dat zijn twee dingen die nu best veel door elkaar gebruikt worden. Wat zit daar dan voor verschil tussen?

Zorginstelling A: Ja, dat kan ik wel uitleggen. Je hebt het grondrecht, artikel 10 mocht je het willen opzoeken is jouw grondrecht op de bescherming van jouw persoonlijke levenssfeer dat betekent dat jij in je huis niet mag worden afgeluisterd, maar ook recht op lichamelijke integriteit, dat niemand zomaar aan je mag zitten. Dat is heel breed gezien jouw recht op privacy. Je mag gewoon in je eigen huis doen wat je wilt, niemand mag je zien, je mag niet worden afgeluisterd of gefilmd. Als je daarop inzoomt op dat hele grote brede privacy dan heb je natuurlijk ook een stukje persoonsgegevens: jij geeft persoonsgegevens aan Facebook of aan Gmail of aan waar je werkt, die verwerkt jouw persoonsgegevens. Die persoonsgegevens moeten ook worden beschermd en daar gaat eigenlijk de Wet Bescherming Persoonsgegevens over, de AVG, wat ik al noemde, dus eigenlijk moet je dat zien als een onderdeel van het hele grote recht op de bescherming van jouw persoonlijke levenssfeer.

RS: Zo had ik het inderdaad ook gezien, maar toch benieuwd hoe jullie daar tegenaan kijken. En in de rest van de organisatie: hoe is de functie daarbinnen? Is er bijvoorbeeld een afdeling voor?

Zorginstelling A: Nee, we hebben geen afdeling. We hebben wel sinds ik ben aangenomen een privacy werkgroep opgetuigd en dat is een kleine groep mensen waaronder dus twee FG's maar ook de informatiebeveiliger. Daar zitten nog twee juristen bij die voor een paar uur per week ondersteuning bieden en we hebben op dit moment nog een communicatiemedewerker dat is ook tijdelijk. Dat clubje is de privacy

werkgroep en daar kunnen mensen terecht voor advies en wij regelen daar zoveel mogelijk in. En die privacy werkgroep hebben we gepositioneerd onder juridische zaken, want het gaat om wetgeving, omdat dat de meest makkelijke manier is of neutrale plek is om deze werkgroep in te zetten. We hebben natuurlijk meerdere afdelingen, bijvoorbeeld medische zaken. Daar zou het natuurlijk onder kunnen, omdat je te maken hebt met patiëntgegevens, maar dan vergeet je eigenlijk weer de medewerkersgegevens, dus dat is dan weer niet helemaal overkoepelend. Dus dit was de meest logische plek.

RS: En hoe is het dan verbonden aan de rest van de organisatie?

Zorginstelling A: Dat valt weer onder de staf. En staf is eigenlijk alle ondersteuning binnen het proces; personeelszaken, relaties alles zit daarin.

RS: Want hoe zijn jullie dan bijvoorbeeld in contact met de communicatieafdeling of met het bestuur, hoe gaat dat in zijn werk?

Zorginstelling A: Als we dus iets met communicatie willen, dan moeten we de afdeling communicatie ook inschakelen bijvoorbeeld. Daar hebben we dan automatisch contact mee en we hebben ook een lijn met de Raad van Bestuur. En wij leveren ook wel rapporten op, zeker naar aanleiding van datalekken, rapportage elke drie maanden.

RS: Ja het is natuurlijk belangrijk om die in beeld te hebben ook. Dus als er dan bijvoorbeeld iets van communicatiebeleid wordt opgesteld waar ligt dan de verantwoordelijkheid? Als iets doorgevoerd moet worden, gaan jullie dan een plan daarvoor maken of is dat?

Zorginstelling A: Uhm nee dat ligt dan bij de verantwoordelijke afdeling, maar wij kunnen daar wel in ondersteunen en aangeven wat daar nodig voor is en advies geven van waar iets moet staan bijvoorbeeld.

RS: Oké.

Zorginstelling A: Als er echt communicatiebeleid moet komen of dat er bepalingen moeten worden opgenomen extra vanuit die verordening, de AVG, dan is het aan het hoofd van die afdeling om onze input mee te nemen.

RS: Oké dus dat wordt dan vanuit daar geregeld en jullie leveren dan input aan.

Zorginstelling A: Ja, precies. Wij zijn niet verantwoordelijk, zeg maar.

RS: En bij het uitvoeren spelen jullie daar enige rol in? Als bijvoorbeeld beleid moet worden doorgevoerd naar medewerkers toe?

Zorginstelling A: In principe moet dat dan via communicatie lopen of via een andere afdeling. We hebben ook beleid P&O bijvoorbeeld dat aangepast moet worden en dan moet die directeur daar ook voor zorgen. Het is wel zo dat ik als FG daarop moet toezien. Ik kan wel op een gegeven moment contact opnemen en eens vragen hoe het ermee staat, dingen controleren.

RS: Ja, precies. Om te kijken of je de dingen die je wilt een beetje terugziet. En nu is het zo dat er afgelopen weken een 'ZEKER' campagne is geweest. Dat is een campagne die erop gericht was om medewerkers bewust te maken van informatiebeveiliging. En ik vroeg me af, waren jullie daar bekend mee met die campagne? En hebben jullie daar misschien iets mee gedaan?

Zorginstelling A: Nee

RS: Op zich een goed initiatief om meer aandacht te creëren voor het onderwerp. Ik las de uitslag en was wel redelijk verbaasd want 97 procent van de medewerkers die had meegedaan die was zich goed bewust van bescherming van persoonsgegevens en dergelijke.

Zorginstelling A: Oh wauw.

RS: dus ik vond dat wel een opmerkelijke uitslag.

Zorginstelling A: Ja.

Maar het was meer gewoon een algemene vraag, want ik was benieuwd of je daar benaderd voor bent. Misschien dat de communicatieafdeling dat wel is. 80 zorginstellingen hebben meegedaan, dus best een groot aantal.

Zorginstelling A: Dat is gewoon van zo'n club als waar jij vandaan komt? Zo'n campagne? Waar komt dat vandaan?

RS: Nou nee, dat is van NVZ, de Nederlandse Vereniging voor Ziekenhuizen is dat volgens mij.

Zorginstelling A: Nou ja misschien dat de afdeling communicatie daar iets van weet, maar ik weet daar niks van.

RS: Ja, alert online, is ook een bekende naam ervan. Nou ja, in ieder geval je kunt het eens opzoeken op internet. Er staan ook wel wat middelen enzo bij die je gewoon gratis kunt downloaden geloof ik.

Zorginstelling A: Oké, handig.

RS: Dan natuurlijk benieuwd of er bij jullie zelf ook beleid is, behalve de 'ZEKER' campagne kan je natuurlijk op allerlei manieren aandacht geven aan privacy. Zijn jullie daar al mee bezig?

Zorginstelling A: Uhm de communicatie daarover?

RS: Onder andere communicatie inderdaad, maar ook de beleidsvoering.

Zorginstelling A: Ja, daar zijn we wel mee bezig. Ja, beleidsvoering wat bedoel je daar precies mee?

RS: Nou je hebt bijvoorbeeld die Wet Meldplicht Datalekken gekregen, daar moet je iets mee. Je moet bijvoorbeeld regels opstellen voor medewerkers. Zijn er zulke regels geformuleerd?

Zorginstelling A: Ah ja zo, ja die zijn er.

RS: Ja en op wat voor manier zijn die geformuleerd. Zijn die gewoon voor alle medewerkers bestemd bijvoorbeeld of spitst dat zich toe op bepaalde groepen?
Zorginstelling A: Nee, we hebben voor datalekken één werkproces gewoon ingericht eigenlijk voor alle medewerkers. Daarvoor hebben wij een telefoonnummer eigenlijk, we hadden al een telefoonnummer dat was de ICT-helplijn. Als jij bijvoorbeeld in de knoei komt met je computer, die doet het niet meer. Die hebben we gevraagd of ze ook de meldlijn willen zijn voor datalekken, bijvoorbeeld als jij in de trein iets verliest dan kan je ook bellen, ook als je dus niet op het werk zit. En ze kunnen meteen daar blokkeren op die afdeling. Daarom hebben we daarvoor gekozen. En dat hebben we breed gecommuniceerd: 'heb je een datalek, bel dit telefoonnummer'.

RS: Dus als er een datalek is of voorkomt of iets dergelijks of misschien dat medewerkers denken dat zoiets gebeurt, dan kunnen ze dus bellen met dat nummer. En dat komt dan bij de ICT-afdeling terecht of bij jullie?

Zorginstelling A: Dat komt, de ICT-medewerker die aan de telefoon zit, die weet, die heeft van ons een vragenlijst gekregen van wat ze moeten uitvragen en daar vullen ze de antwoorden in en dat sturen ze naar ons toe. Wij doen de beoordeling en dat komt dan naar ons toe. Dan pakken wij het op. Wij doen de beoordeling, de FG's dan, of het ook bij de autoriteit persoonsgegevens gemeld moet worden bijvoorbeeld. En of er maatregelen genomen moeten worden om het in de toekomst weer te voorkomen.

RS: Ja, wie weet moet het beleid aangepast worden

Zorginstelling A: Ja, dat houden we bij, al die meldingen staan in het register.

RS: Is dat dan naar alle medewerkers gegaan of alleen artsen of verpleegkundig personeel?

Zorginstelling A: Nee, naar alle medewerkers.

RS: En die melding van dat dat telefoonnummer er is, op wat voor manier is dat dan gegaan?

Zorginstelling A: Dat hebben we gedaan met een brief, dat is dan van de Raad van Bestuur, dat is een brief die gaat dan de hele organisatie door. Uh, en we hebben een intranet daar heeft het opgestaan. Daarin hebben we ook gecommuniceerd. Onze eigen intranetpagina, waar we ook uh, daar informatie hebben en vragen van: wat is nu een datalek en wanneer moet je dan bellen en dat soort dingen. We hebben nog een flyer, ja we hebben nog wel wat flyers gemaakt. Ik heb nog wel wat meegenomen.

RS: Oké ik ben benieuwd.

Zorginstelling A: Daar hebben we in die zin wel aandacht aan besteed. En we hebben ook, ja dan heb ik hier niet echt een goed voorbeeld van maar we hebben dergelijke dingen ook wel gewoon opgehangen: Datalek: bel. We hebben ook wel op bepaalde afdelingen presentaties gegeven.

RS: En wat voor afdelingen zijn dat dan bijvoorbeeld waar presentaties worden gegeven?

Zorginstelling A: oh dan moet ik even nadenken.

RS: Nou ja wat voor soort afdelingen?

Zorginstelling A: We zijn wel bij verpleegkundigen overleg geweest bijvoorbeeld. Ja, beetje wel echt van die zorgafdelingen. Ik weet niet precies meer welke allemaal. Vaak wel een beetje op verzoek ook hoor, zo van: nou we willen nog wel wat extra informatie, we hebben die brief gelezen maar we snappen het nog niet helemaal.
RS: En heb jij die presentaties dan verzorgd of werden die verzorgd door bijvoorbeeld communicatie?

Zorginstelling A: Nee, dat is wel vanuit de privacy werkgroep verzorgd. En ook dit soort communicatiedingetjes (laat campagnetitel: 'Wat zou jij doen?' zien). Dit is bijvoorbeeld een campagne geweest voor de datalekken. Dit werd dan opengesneden met wat zou jij doen en daarachter stond dan een situatie beschreven. Bijvoorbeeld: Nou er ligt een dossier op de balie, wat zou jij doen? Om een beetje mensen te prikkelen zo van denk er eens over na.

RS: Ja, precies. En dit is dan een voorbeeld van hoe dat eruit ziet?

Zorginstelling A: Ja en dit verspreiden we dan over het hele ziekenhuis.

RS: Oké dus dan zie je dat ergens hangen en dat je erover na gaat denken?

Zorginstelling A: Ja, dan zie je dat en dan kijk je onder het flapje. De situatie staat onder het flapje met bovenop de vraag, wat zou je dan doen?

RS: Oké dus je moet hem eerst omslaan en dan kan je dat lezen en het antwoord staat dat er ook bij of?

Zorginstelling A: Nee, nee dat moet je zelf bedenken. En die kwam op een gegeven moment op intranet. En dit heb ik zelf getekend ook toevallig.

RS: Oh, dan kun je mooi tekenen dan. En mag ik dat meenemen eventueel?

Zorginstelling A: Ligt eraan wat je ermee gaat doen.

RS: Ik heb meer, wat ik ermee ga doen, is gewoon als extra documenten er naast leggen om bijvoorbeeld nog extra informatie toe te kunnen voegen. Ik heb bijvoorbeeld nu gezien er is een bewustwordingscampagne geweest en je geeft ook heel duidelijk voorbeelden van waar het precies hangt, maar om nog iets meer inhoudelijk te kunnen kijken. Zodat ik bijvoorbeeld kan beoordelen: is dit meer informatief of meer bewust maken.

Zorginstelling A: Op zich mag je het wel mee, maar je mag het niet publiceren.

RS: Nee, snap ik.

Zorginstelling A: Er staan ook voorbeelden van datalekken op bij ons bijvoorbeeld. Dit is een overzicht van zes maanden datalekken.

RS: Oké en dat hing dan wel ergens?

Zorginstelling A: Meer dat we mensen wilden informeren van nou wat hebben we nu allemaal hoe kun je dat voorkomen met de informatie waar je dat moet melden.

RS: Oké dus hier staan ook wel gevoelige gegevens op?

Zorginstelling A: Ja.

RS: Oké dus dat is meer intern gebeurd? Dat hing ook niet in de openbare ruimten neem ik aan.

Zorginstelling A: Ja bij personeelskamers, bij printers. Nee, maar dit ook niet (bewustwordingscampagne) dit is ook bij personeelskamers, dit is voor medewerkers bedoeld natuurlijk niet voor patiënten.

RS: Nee, maar je kan je voorstellen bijvoorbeeld dat het in de gangen hangt.

Zorginstelling A: Nee, nee.

RS: Oké dus dit moet ik zien als een soort overzicht van de gemelde datalekken en hoe die dan oja ik lees hier: wist je dat en hoe die gekomen zijn.

Zorginstelling A: Bewustwording ook van goh wat gebeurt er nou en hoe kan je dat voorkomen. Om mensen weer aan het denken te zetten van goh oh dat is inderdaad wel herkenbaar. Of oja hier kan ik nog wel wat beter over nadenken of beter op letten.

RS: Nee, precies. Nou dan weet ik in principe genoeg hoor, dan hoef ik dit ook niet mee te nemen. Dan is dat prima. Nee, het was gewoon meer om informatie te hebben van waar gaan die campagnes nu over, meer over de inhoud van campagnes.

Zorginstelling A: En deze hebben we ook nog. Dit is een checklist informatiebeveiliging en privacybescherming. En die was er al voor informatiebeveiliging, maar die hebben we dus uitgebreid met privacydingen en ook met de Meldplicht Datalekken.

RS: Oké

Zorginstelling A: dus dit wordt aan alle medewerkers verstrekt.

RS: Ook als er nieuwe medewerkers komen?

Zorginstelling A: Ja, vooral. Ja, meldt mijn datalek staat hier. En nummers voor waar je dan heen moet bellen.

RS: Oké dus dat is meer een soort checklist. Staan daar gevoelige dingen op?

Zorginstelling A: Nee, maar ja dit is wel van de zorginstelling specifiek natuurlijk met ook onze interne telefoonnummers.

RS: Oja, ik heb dit soort documenten wel vaker gezien en dan ook niet in het onderzoek gebruikt verder. Jullie hebben er een checklist voor en dit zijn de verschillende onderwerpen en één daarvan is datalekken.

Zorginstelling A: Ja hier staan ook dingen in als: log je computer uit als je even naar het toilet gaat of als je even wegloopt. Dat je het niet open laat staan.

RS: Oké dus ook wel checklist van op je werkplek.

Zorginstelling A: Ja, ja, ja.

RS: Oké dus dan staan er dingen waar je rekening mee moet houden op je werkplek?

Zorginstelling A: Ja, dat mag je wel lezen.

RS: even kijken hoor. Ja wachtwoorden inderdaad. Was inderdaad ook één van mijn vragen of er een wachtwoordbeleid is, dat is er duidelijk te zien en hoe je om moet gaan met patiëntgegevens. Maar het is inderdaad belangrijk dit soort dingen onder de aandacht te brengen.

Zorginstelling A: Ja, wat we ook nog doen is we hebben elk jaar de dag van de patiëntveiligheid. En dan heb je allemaal standjes die allemaal met patiëntveiligheid te maken hebben en dan hebben wij ook een stand. En dan brengen we bijvoorbeeld die datalekken weer onder de aandacht.

RS: En dan iedereen van de medewerkers komt daar of wordt dat opgedeeld?

Zorginstelling A: Het is heel groot, een soort van dorp met straten daarbinnen en in de grote straat is het dan met allemaal kraampjes, dat wordt groots aangekondigd van tevoren van de dag van de patiëntveiligheid kom allemaal kijken. Nou daar staan dan kraampjes. En we hebben ook vaak wel een bijeenkomst voor medewerkers. Vorig jaar hadden we iemand die ging vertellen over wat kan identiteitsfraude allemaal wat kan ermee gebeuren hoe erg is dat en iedereen schrikt zich dan rot natuurlijk. En we hebben er weer één in november, dan hebben we een hacker die gaat laten zien hoe en wat we allemaal een beetje aan het lekken zijn. Om ook, ja de bewustwording vooral dus weer te stimuleren zeg maar.

RS: En worden dit soort ideeën dan meestal door jullie bedacht of hoe gaat dat bijvoorbeeld vanuit de Raad van Bestuur hebben zij dat thema ook een beetje goed in beeld?

Zorginstelling A: Uhm, nee wij initiëren dit zeg maar, maar die brieven die wij de organisatie sturen, die gaan wel langs de Raad van Bestuur en ook onze rapportages datalekken. En de Raad van Bestuur heeft natuurlijk wel ingestemd met het oprichten van de privacywerkgroep en met het aannemen van mij als extra functionaris van de gegevensbescherming, dus in die zin is er wel enigszins bewustzijn. Voor mijn gevoel kan het altijd meer.

RS: Ja, is natuurlijk ook er zijn zat thema's waar je mee bezig kunt houden als bestuur, maar ik vroeg me af in hoeverre zij er ook zelf mee bezig zijn. Ja in hoeverre zij het in beeld hebben ook, staat het bijvoorbeeld op de agenda.

Zorginstelling A: Ze hebben natuurlijk allemaal hun eigen portefeuille ook, dus er is één die dat in zijn portefeuille heeft en dat op zich ook wel belangrijk vindt, de anderen hebben daar iets minder feeling mee. Je hebt sowieso met zoveel mensen te maken, de één vindt het heel belangrijk, de ander vindt het irritante onzin, ja.

RS: Ja, dat heb je toch in de maatschappij ook: je gaat ook niet al die verklaringen lezen van Google.

Zorginstelling A: Nee, nee. Wat heel leuk is om ook nog te vertellen. Dat hebben dan trainees gedaan die wij ook bij de privacywerkgroep hadden. Die hebben belevingsonderzoek gedaan binnen de organisatie. Er hebben een paar stagiaires meegelopen in het primair proces met verpleegkundigen. Kijken: wat doen ze eigenlijk en een beetje het gesprek aangaan: laat maar zien wat je doet en wat kom je nu tegen als je denkt aan privacy, waar denk je dan aan? Wat voor dilemma's heb je dan in je werk? Want we willen ook wel graag dat het werkbaar blijft. Om zo mensen daarover na te laten denken.

RS: Oké dus ook wel inderdaad op de werkvloer ermee bezig.

Zorginstelling A: Nou niet alleen in de zorg, maar ook logistiek. Op alle soorten.

RS: Oké dat is wel interessant inderdaad.

Zorginstelling A: Ja, dat is wel heel leuk en daar hebben we ook wel wat ambassadeurs aan over gehouden, mensen die echt wel enthousiast zijn.

RS: Ja, dat is echt een grappige manier. Het is ook een beetje een manier om barrières op te lossen misschien in een later stadium?

Zorginstelling A: Ja, ja.

RS: Want jullie hebben dan bijvoorbeeld dit gedaan, zo'n voorbeeld van een flyer en die campagne. Wordt dat dan in de tussentijd geëvalueerd?

Zorginstelling A: Uhm.

RS: In hoeverre mensen daarin hun gedrag misschien aangepast hebben? Ja of iets werkbaar is? Je krijgt misschien wel eens vragen.

Zorginstelling A: Ja, dat sowieso. En dat belevingsonderzoek is afgerond en we daarna heeft de trainee nog klinische lessen gegeven en nog wat meer informatie over wat betekent dat nu allemaal en zo gaan we een beetje de organisatie wel door. En nu ook op andere plekken, want we hebben ons eerst gericht op het primair proces dus de zorg zeg maar. En nu gaan we ook kijken naar onze andere domeinen, zoals bedrijfsvoering waar de medewerkersgegevens liggen, maar ook onderzoek en onderwijs, ook een belangrijke. Maar echt evalueren, nee.

RS: Nee, daar is het misschien ook nog een iets te vroeg stadium voor.

Zorginstelling A: Misschien wel.

RS: En is er bijvoorbeeld ook externe mogelijkheid om dingen te melden? Je hebt natuurlijk ethische hackers of iets dergelijks. Kunnen die via de site ook dingen melden? Of iemand die iets opvalt?

Zorginstelling A: We hebben voor extern nog niet een datalekportaal maar op zich willen we dat wel, dus we zijn daar wel mee bezig. Omdat bijvoorbeeld mensen ook wel eens een verkeerde brief krijgen, met bijvoorbeeld patiëntgegevens daarop van een ander. Dus dat is vrij vreselijk natuurlijk. En meestal komt dat wel bij ons binnen via de afdeling waar diegene onder behandeling is of dan belt die afdeling zeg maar ons nummer, maar eigenlijk willen we ook gewoon dat die mensen rechtstreeks iets kunnen melden. Nou hebben we wel een algemene plek: we hebben op onze website natuurlijk gewoon contact, maar we hebben ook meld het ons of bel ons knop waar mensen eigenlijk alle opmerkingen of feedback over alles wat ze maar kwijt willen over de instelling kwijt kunnen.

RS: Oké en dat wordt dan gefilterd of iets dergelijks?

Zorginstelling A: Ja dat is dus heel algemeen. Dat komt terecht bij baliemedewerkers.

RS: Oké dus dat zou wel iemand kunnen doen in theorie (melden via de website), maar dan is het misschien nog best lastig inderdaad. Niet dat er zeg maar rechts bovenin staat van 'meldpunt'.

Zorginstelling A: Nee, dat hebben we dus nog niet, maar we hebben die behoefte op zich wel. Maar dat is de volgende stap.

RS: Ja, ik ben benieuwd of daar veel respons op zou komen. En ik vroeg me ook af want artsen die zijn natuurlijk een belangrijke groep, tenminste als je iets in het nieuws hoort, zijn het vaak artsen die iets mee naar huis hebben genomen en dan liggen er weer van allerlei gegevens op straat of in de trein of wat je ook maar hoort. Hoe ga je met die groep om, want ik kan me voorstellen dat dat best een lastige groep is.

Zorginstelling A: Ja, dat klopt wel. Dat is ook wel een lastige groep. Ja we nemen ze natuurlijk mee in de algemene campagnes. We hebben in ieder geval nog een student onderzoek laten doen binnen die groep naar hun intrinsieke motivatie om te voldoen aan dit soort wettelijke dingen. Even denken.

RS: Wat zou hen dan bijvoorbeeld motiveren om mee te doen?

Zorginstelling A: Er is wel intrinsieke motivatie om het geheim te houden, want dat hoort bij hun beroep. Maar meer intrinsiek dan vanuit dat ze weten hoe het werkt in de wet, zeg maar.

RS: En hoe zit dat dan bijvoorbeeld bij de Raad van Bestuur hebben zij er een soort van zicht op wat het risico is van een datalek?

Zorginstelling A: Ja, dat hoop ik, maar dat weet ik niet zo goed of ze dat hebben. Sowieso zit er voor artsen nog een specifiek risico dat ze hun geheimhouding kunnen breken en dat ze dan voor een tuchtrechter worden gedaagd. En persoonlijk aansprakelijk worden gesteld, maar goed datalekken algemeen: je meldt het bijvoorbeeld niet, je komt toch in het nieuws of je neemt niet genoeg beveiligingsmaatregelen kun je ook vrij hoge boetes voor krijgen. Wij geven dat natuurlijk wel aan.

RS: Ik ben meer benieuwd of ze dan inderdaad reputatie als een belangrijke factor zien of het risico op boetes of iets anders?

Zorginstelling A: Nee, dat weet ik niet. Ik sta dan toch iets te ver van de Raad van Bestuur af om dat te weten hoe zij ernaar kijken, dat weet ik eigenlijk ook niet zo goed.

RS: Ja het zou kunnen dat ze het terugkoppelen aan afdelingen bijvoorbeeld we zijn nu hier en hier mee bezig.

Zorginstelling A: Nee, nee. Het belang wordt wel erkend, maar hoe ze er precies naar kijken dat durf ik niet te zeggen.

RS: En als je dan kijkt naar de communicatie in hoeverre denk je dan dat dat bij kan dragen aan het inperken van de risico's?

Zorginstelling A: Heel veel. Het grootste probleem met datalekken is het menselijk handelen, dus daar heb je het meest de medewerker gewoon bij nodig en die moet bewustzijn van wat ie doet, wil hij ook iets kunnen doen. Als je niet weet wat je aan het doen bent of als je onbewust gegevens aan het lekken bent of er gewoon slordig mee omgaat en bewust je computer niet afsluit of een scherm open laat staan in een vergaderruimte, waar dan nog patiëntendossiers openstaan terwijl de volgende club binnenkomt. Ja, als mensen daar niet bewust van zijn dan kun je daar ook heel weinig mee. Mensen bewustmaken, dus we zijn heel erg bezig met dat bewustzijn. En ook die datalekken helpen, want dat koppel je natuurlijk terug aan die afdeling: hee dit

gebeurde er. Oh chips, nee dat mag natuurlijk niet en oh wat vervelend en daar gaan we meteen aan werken. Vaak wordt er dan in teamoverleg ook weer aandacht aan besteed dat er extra weer op gelet moet worden.

RS: Oh ja, en is het dan ook zo dat bewustwording meer komt nadat er een datalek is voorgekomen of?
Zorginstelling A: 'Ja dat helpt wel ja. Wij hadden laatst ook een datalek.

RS: Zijn dat dan momenten waarop je daarna ziet van mensen zijn er meer mee bezig dan daarvoor?

Zorginstelling A: Ik denk het wel.

RS: En bijvoorbeeld de Meldplicht Datalekken ging natuurlijk in op 1 januari en was dat dan ook een moment dat mensen er vanaf toen ineens meer mee bezig waren of anders mee bezig waren. Want jij bent natuurlijk al twee jaar geleden zei je aangesteld?

Zorginstelling A: Ja, we moesten wel. Ja, voor 1 januari heb ik het proces al opgesteld en de communicatie ook gestart en ook aangegeven dat we nog een periode wilden oefenen als het ware. Vanaf oktober: begin maar met melden ook al is het nog niet officieel, dus we hebben eigenlijk vanaf oktober al meldingen gekregen, dat wordt wel meer.

RS: Oké dus wel op geanticipeerd.

Zorginstelling A: Ja, want we moeten natuurlijk zelf ook leren wat je dan voor dingen krijgt en hoe je dan een melding plaatst.

RS: ja, dat is ook zo. En krijgen jullie nu over het algemeen veel meldingen binnen op een dag?

Zorginstelling A: Nou dat wisselt heel erg, ongeveer vier per week. Maar dat kunnen soms dus vier op een dag zijn en soms ook in een week één.

RS: En bijvoorbeeld je hebt natuurlijk 72 uur om goed dat in kaart te brengen na dat punt dat je het ontdekt hebt en als er dan een weekend of zoiets tussen zit?

Zorginstelling A: Nou dat is nog lastig. We hebben daar eigenlijk te weinig capaciteit voor als FG. We hebben het wel zo gedaan dat de helplijn 24 uur bereikbaar is, dus als er echt iets ergs is, dan kan de meldlijn gebeld worden. Dan wordt het opgepakt. Stel er moet iets worden geblokkeerd, dan kan dat ook meteen worden gedaan en dan in principe is het wel zo dat de directeuren weekenddienst hebben, dan hoop ik dat er een directeur gebeld wordt, maar dat is nog niet helemaal officieel. Ik heb dat nog niet helemaal rondgekregen.

RS: Ja, want het is bijvoorbeeld als je kijkt naar het crisiscommunicatieplan, heb je vaak op de communicatieafdeling dat mensen ook in het weekend opgeroepen kunnen worden voor bepaalde dingen.

Zorginstelling A: We hebben dat nog niet goed voor elkaar gekregen om dat echt vast te leggen, omdat de directeuren daar ook niet altijd zin in hebben. En wij ook eigenlijk te weinig uren hebben om dat te kunnen.

RS: Ja, oké en er wordt natuurlijk ook voor zo'n campagne budget vrijgemaakt, kan ik me voorstellen. Kun je het daarin terugzien dat er wat meer budget vrijkomt voor dit soort thema's?

Zorginstelling A: Nee, volgens mij dit weet ik niet precies, volgens mij krijgt de privacywerkgroep wel een bepaald budget.

RS: en dat is dan ook bijvoorbeeld waar je de communicatie weer vanuit moet betalen?

Zorginstelling A: Ja, en dat moet zo min mogelijk. Het is volgens mij vooral budget voor de medewerkers. En extra we proberen heel veel dingen toch wel in de lijn te beleggen, omdat daar ook de verantwoordelijkheid ligt.

RS: Ja, dus dat is ook nog best lastig eigenlijk. Jij bent nu natuurlijk met één collega en de weekenden zijn nog een lastig moment.

Zorginstelling A: Nee, we kunnen geen 24-uursdiensten draaien dat mag ook niet verwacht worden met ons aantal uren, dat is heel simpel. Dus we halen het niet altijd. En ja wat vrijdag binnenkomt dat pakken we maandag weer op in principe. Dan ben je nog wel net op tijd, maar daar kan nog wel wat verbeteren.

RS: Daar zou op zich wel wat meer aandacht voor kunnen zijn dus. Natuurlijk vanuit de privacyhoek: hoe meer aandacht hoe beter. Vond ik wel interessant aan dit thema, ik heb zelf ook geen juridische achtergrond, om te zien hoe dit nu zo enorm leeft ook in de media. Het is ook onderzoek naar onderzoek wordt erover gepubliceerd. Nog niet toen wij hiermee begonnen, want we hebben natuurlijk in mei dit thema vastgesteld. En ineens na de zomer, vanaf september werd er enorm veel aandacht aan besteed bijvoorbeeld de autoriteit persoonsgegevens als waakhond. En de autoriteit persoonsgegevens is natuurlijk ook wel een belangrijke instantie, want ben je bijvoorbeeld ook verbonden aan die vereniging, de Nederlandse Vakbond voor Functionarissen van de Gegevensbescherming.

Zorginstelling A: Ja, ik niet, maar mijn collega wel.

RS: Oké ik ben dus naar een bijeenkomst van hen geweest, daar was ook de Autoriteit Persoonsgegevens aanwezig, want ik vroeg me af: hoe kijk je nu tegen de rol van de Autoriteit Persoonsgegevens aan?

Zorginstelling A: Ja vooral als externe toezichthouder.

RS: Krijg je soms ook bijvoorbeeld berichten van hen waar je iets aan hebt misschien?

Zorginstelling A: Nee, nee. Ze zitten wel op afstand zeg maar.

RS: Want ja ik kan me voorstellen dat je met vragen zit op een gegeven moment over bepaalde zaken.

Zorginstelling A: Ja, maar ik weet dat zij daar geen antwoord op gaan geven, want ze willen heel erg de toezichthouder zijn en geen advies geven of ergens op in gaan.

RS: Nee, daar hebben ze inderdaad bewust voor gekozen.

Zorginstelling A: In mijn ervaring vind ik ze niet heel benaderbaar en ook als FG van een organisatie ook niet uitnodigend, want het is een toezichthouder, dus als je daar je vraag gaat stellen, krijg je misschien ook wel weer op je dak.

RS: Ja, dat is een beetje hetzelfde wat ik merkte bij de sfeer van die bijeenkomst, niemand zei echt van welke organisatie hij of zij was.

Zorginstelling A: nee, dat kan ik me wel voorstellen.

RS: Udo Oelen was er van de autoriteit persoonsgegevens, hij deed wel erg zijn best. Was ik in ieder geval positief door verrast. Ik hoorde zelf ook vaker terug inderdaad dat de Autoriteit Persoonsgegevens heel erg op afstand bleef. Hij probeerde dat wel te doorbreken, maar je hebt dan natuurlijk maar twee uurtjes, dus dan is het lastig. Nou extern melden hebben we het over gehad, dat is er nog niet echt. Die lijn kun je natuurlijk ook als extern persoon bellen.

Zorginstelling A: Je hebt van de Autoriteit Persoonsgegevens natuurlijk ook een meldformulier op internet en daar vul ik het op in. De meldingen doe ik en mijn collega FG.

RS: en er is wel genoeg informatie? Want hoe gaat dat dan bijvoorbeeld? Iemand meldt dat, wordt diegene dan betrokken bij het proces? Wordt diegene daarin meegenomen?

Zorginstelling A: Nou ja, ik bel vaak nog wel even terug naar diegene, want heb vaak nog wel wat extra informatie nodig, zoals wat er nou precies gebeurd is.

RS: Ja, dat formulier is erg uitgebreid.

Zorginstelling A: Ja, vaak informeer ik de melder wel of ik het meld. En ook vaak de leidinggevende van de afdeling, hee dit is een datalek geweest, die ik ook heb gemeld bij de Autoriteit Persoonsgegevens, maar wat daar gebeurt daar heb ik geen zicht op he. Ik stuur het weg en dat is het.

RS: Ja, dat werd wel een beetje uitgelegd op die bijeenkomst, hoe ze dat een beetje doen. Ja, dat is misschien voor een andere keer weer. Ja hoe ze dat een beetje aanpakken, dus dat was wel interessant natuurlijk hoe ze dat aanpakken.

Zorginstelling A: Ja, ik heb er wel een verslag van gelezen.

RS: Ah, oke.

Zorginstelling A: Toevallig via de instantie waar ik de opleiding tot FG volg.

RS: Dat is dan voor de functie FG?

Zorginstelling A: Ja, echt de leergang FG voor twee jaar.

RS: Oh, die bestaat al twee jaar. Oké dat vind ik interessant.

Zorginstelling A: Of die twee jaar bestaat, durf ik niet te zeggen, maar de opleiding duurt twee jaar en ik ben nu anderhalf jaar bezig.

RS: Dat is een interessante, want er is ook een opleiding die ik ken van IIR. En daar heb je dus een opleiding voor Certified Data Protection Officer. Dat is eigenlijk hetzelfde maar dan met een Engelse term.

Zorginstelling A: Hoe lang duurt die opleiding dan of hoe groot is dat dan ongeveer?

RS: Ja, het is dan een paar dagen steeds. Het gaat in stukjes. Je krijgt er af en toe huiswerk van mee of een toets over. Heel veel thema's komen aan bod van beveiliging tot communicatie, want de Europese Verordening van 2018 die komt er natuurlijk ook aan.

Zorginstelling A: Nee, die is er nu al hè.
RS: Oh, is die er al?

Zorginstelling A: Jij bedoelt de AVG? Die is 25 mei 2016 is die van kracht geworden, alleen twee jaar krijgen organisaties de tijd om eraan te gaan voldoen en dan in mei 2018 kan de Autoriteit Persoonsgegevens ook gaan handhaven. Dus vanaf dat moment kan de autoriteit ook boetes uit gaan delen binnen deze wet. Maar hij geldt nu al, dus je moet er al wel aan voldoen.

RS: Oké want je kunt nu toch al wel boetes opgelegd krijgen vanuit de Autoriteit Persoonsgegevens?

Zorginstelling A: Ja, dat klopt maar dat is geregeld vanuit de Wet Meldplicht Datalekken, daar is de boetebevoegdheid groter gemaakt. Niet alleen voor datalekken, maar ook voor andere bepalingen. Dat is een bepaald bedrag, een bepaalde grens en de AVG heeft weer een andere grens en die is handhaafbaar vanaf 2018 en daarin staat bijvoorbeeld dat je documentatieplicht hebt, dat je daaraan moet voldoen, dus de organisaties moeten er nu aan gaan voldoen, maar over twee jaar pas kunnen ze daar een boete voor krijgen als ze dat dan nog niet op orde hebben.

RS: Oh, oké, dus je hebt nu eigenlijk een soort tussenperiode, waar je twee jaar hebt.

Zorginstelling A: Ja, een overgangstermijn in feite.

RS: En in hoeverre denken jullie dan dat jullie daar klaar voor gaan zijn?

Zorginstelling A: Wij doen hard ons best om daar klaar voor te zijn. Nee, dat is moeilijk te zeggen. Het is niet op één dag geregeld.

RS: Nee, maar er is een soort stappenplan?

Zorginstelling A: Ja.

RS: Oké dat vind ik wel interessant, want dat heb ik dus niet zo begrepen op de congressen waar ik geweest ben. Daar hadden ze het de hele tijd over die mei 2018 en dat die Europese Verordening dan van start ging.

Zorginstelling A: Oja.

RS: Oké volgens mij heb ik al mijn vragen gesteld, ik zal het nog even checken. Voor mijn gevoel heb ik in ieder geval een heleboel nieuwe informatie, maar toch altijd even checken dat ik wel alle informatie heb. Hartstikke bedankt voor het interview. Ik zal het interview eerst wel even naar jou toesturen om te kijken of het zo in het onderzoek kan worden meegenomen.

5.2 Uitwerking interview zorginstelling B

Uitwerking interview zorginstelling B Ziekenhuis

In het voorgesprek werd ook aandacht geschonken aan de 'ZEKER' campagne van NVZ daar begon de geïnterviewde over, hij vond dit niet zo'n sterke campagne.

RS: Eerst eigenlijk benieuwd. Hoe ben je zo bij deze functie terechtgekomen? Het is natuurlijk vrij nieuw dat elke instelling dit moet hebben een functionaris van de gegevensbescherming.

Zorginstelling B: volgens mij is het nog niet verplicht.

RS: nog steeds niet verplicht?

Zorginstelling B: Volgens mij niet. Het zou verplicht worden, maar ik weet het niet. Maar ja hoe is dat gekomen, ja, dat is bijna een toevalsverhaal zeg maar. Op een gegeven moment ben ik gevraagd door de organisatie om risicomanager te worden en toen speelde het al dat het verplicht zou gaan worden dat er een functionaris gegevensbescherming zou komen en toen is ja hoe moet ik dat nou zeggen dat daarin gezet zeg maar in de functie van risicomanager.

RS: Oké dus het is daar onderdeel van? En hoeveel uur per week ben je er dan zo ongeveer mee bezig?

Zorginstelling B: Ja, dat vind ik heel erg lastig. De ene week veel meer dan de andere. Maar ook weer niet zo heel erg veel, want dat moet ik er wel bij zeggen. Kijk ik ben een functionaris gegevensbescherming, maar als je kijkt naar de competenties zeg maar, dan zou dat toch iemand moeten zijn met een uitgebreide wetskennis en nou weet ik ondertussen uit ervaring een hele hoop, maar ik heb daar geen opleiding voor. Maar daar spar ik dan heel veel mee met de jurist van het ziekenhuis, de secretaris Raad van Bestuur, dus in die zin doen we het ook wel een beetje samen zeg maar.

RS: Ja, ja precies.

Zorginstelling B: Als het echt over wetskennis gaat of dat soort dingen dan doet hij het met name en de meer operationele dingen die doe ik dan.

RS: Oké

Zorginstelling B: Dus zo hebben we het een beetje verdeeld en ja hoe lang zal ik daar mee bezig zijn drie vier uur in de week, zoiets, een dagdeel denk ik gemiddeld.

RS: Oké en is dit dan onderverdeeld onder bijvoorbeeld de ICT-afdeling of hoe zit dat? Hoe liggen die verhoudingen?

Zorginstelling B: Nee, ik val rechtstreeks onder de Raad van Bestuur.

RS: Oké en uhm heb je daar dan ook vaak contact mee om dingen te bespreken?

Zorginstelling B: Ik heb met de beide leden van de Raad van Bestuur, dat komt ook omdat ik een gedeelde functie heb zeg maar, maandelijks contact.

RS: oké en worden er dan bijvoorbeeld ook gevallen besproken als er iets voorkomt of?

Zorginstelling B: Als dat nodig is, ja.

RS: En rapporten of iets dergelijks?

Zorginstelling B: Ja, zo gauw als er informatiebeveiligingsincidenten zijn, hebben wij daar zeg maar een commissietje voor die dat onderzoekt. Dan ben ik degene die dat praktisch onderzoekt en dan maak ik een rapport. Dat stuur ik naar die andere twee leden. Dat bespreken we dan eerst even samen en dat gaat altijd naar de Raad van Bestuur.

RS: Oké het gaat dus eerst altijd langs de Raad van Bestuur ook als er bijvoorbeeld een melding wordt gedaan van een datalek of een mogelijk datalek voordat bijvoorbeeld de Autoriteit Persoonsgegevens wordt ingelicht?

Zorginstelling B: Ja.

RS: Oké dus die zijn daar dan uiteindelijk…

Zorginstelling B: Kijk als het een onderzoek is naar een datalek dan maken wij een rapportje hè in de praktijk is het dan meestal zo, ik maak het rapport en die anderen die lezen mee en geven op of aanmerkingen daarop en in dat rapport staat dan het advies voor de Raad van Bestuur; het wel of niet melden, de betrokkene melden dat staat daar.

RS: Oké en dan kunnen zij uiteindelijk beslissen of zij dat gaan doen?

Zorginstelling B: Ja.

RS: Dus de verantwoordelijkheid ligt dan bij de Raad van Bestuur?

Zorginstelling B: Ja, volgens mij is dat per definitie zo.

RS: Ja, dat ligt eraan als jij als functionaris gegevensbescherming natuurlijk een onafhankelijke functie hebt.

Zorginstelling B: Ja, ja ik heb een onafhankelijke functie dat is zeker zo. Maar de Raad van Bestuur is ook hoofdelijk aansprakelijk op het moment dat het fout gaat.

RS: Ja, dat is natuurlijk zeker zo.

Zorginstelling B: Dus vind ik het heel logisch dat zij degene zijn die daar het eindoordeel over vellen.

RS: Ja, en hebben zij dan ook een beetje in beeld hoe dat binnen jullie organisatie speelt?

Zorginstelling B: Ik denk dat, er zijn afgelopen jaar echt wel een paar rapporten geschreven zeg maar, ja, dan krijg je ook een beeld over hoe dat gaat in de organisatie en dat wij één van onze bestuurders werkt hier al twaalf jaar. Ja, ik denk wel dat die een beeld hebben.

RS: En kiezen zij er dan ook voor om beleid te maken voor bijvoorbeeld medewerkers omtrent dit thema?

Zorginstelling B: Ja, dat gaat in de praktijk niet zo hè. Kijk dat beleid dat wordt gemaakt door de mensen onder de Raad van Bestuur onder andere door mij. En zij uiteindelijk fiatteren dat.

RS: Ja.

Zorginstelling B: Zo gaat dat hè, wij doen een voorstel en natuurlijk kijken zij daar nog wel overheen van zijn we het daar helemaal mee eens, maar zij stellen het uiteindelijk vast zo gaat dat.

RS: Ja, maar het komt niet vanuit hen bijvoorbeeld van hier moeten we aandacht aan gaan besteden dit jaar: verzin hier iets voor.

Zorginstelling B: Nee, eigenlijk komt dat nauwelijks voor. Dat gaat andersom.

RS: Oké, dat is grappig.

Zorginstelling B: Dat gaat vaak andersom. Wij komen met voorstellen van hier zouden we aandacht aan moeten besteden en dat adviseer je dan en dan wordt dat door hen besloten.

RS: Oké

Zorginstelling B: Zo gaat dat in de praktijk.

RS: En hebben jullie dan ook de afgelopen jaren iets van beleid opgesteld omtrent dit thema?

Zorginstelling B: Ja, wij hebben een privacybeleid. Dat heeft volgens mij ieder ziekenhuis wel. Maar we hebben ook procedures opgesteld rondom die datalekken. Daar is ook communicatie over geweest naar de organisatie toe. We hebben ook een loginbeleid opgesteld bijvoorbeeld van hoe doen we dat nou? Ja, ja, dus er is van alles.

RS: En maken jullie dan bijvoorbeeld ook onderscheid tussen verschillende groepen in het ziekenhuis? Want je hebt natuurlijk verschillende groepen je hebt natuurlijk stafmedewerkers en je hebt natuurlijk artsen, verpleegkundigen. Worden die groepen ook anders benaderd misschien?

Zorginstelling B: Tuurlijk. Ik weet niet precies wat je dan bedoelt, maar bedoel je in de communicatie?

RS: Ja en ook wel natuurlijk in het beleid.

Zorginstelling B: Kijk in het beleid is het natuurlijk anders, want wat je mag en wat je kan zeg maar is afhankelijk van je functie. In de communicatie, kijk communicatie moet je in feite opsplitsen hè. Je doet een algemene communicatie het huis in. We hebben hier zo'n weekblaadje en daar staat dan ook af en toe wat in over wat we constateren of waar we vinden dat aandacht aan besteed moet worden. Dat is geheel generiek.

RS: Ja.

Zorginstelling B: Maar wat ook gebeurt is dat je via de lijn communiceert, omdat je bepaalde groepen beter wilt bereiken zeg maar. Dan maak je onderscheid, dus dat is heel afhankelijk van waar je het over hebt.

RS: Ja. En bijvoorbeeld dan bij de datalekken meldplicht toen die in ging hoe ging dat?

Zorginstelling B: Dat is geheel algemeen gegaan, dus iedereen dezelfde communicatie en dat is langs twee sporen gegaan. Dus dat is in het algemene nieuwsblaadje van het ziekenhuis gegaan uhm, maar ook via het MT de organisatie in dus via de lijn omdat een datalek in feite overal in de organisatie kan voorkomen. Dat wordt wel eens vergeten hè, want iedereen denkt altijd aan patiëntengegevens.

RS: Ja, er zijn ook medewerkersgegevens.

Zorginstelling B: Precies.

RS: Is wel één van de redenen om eerst in dit onderzoek focus op de zorg te leggen, omdat het misschien wel iets meer betekenis voor de organisatie heeft.

Zorginstelling B: Ja, dat is wel zo. In die zin ben ik het daar helemaal mee eens en aan de andere kant is dat ook meteen een valkuil. Want iedereen als we het over privacy hebben, dan denkt iedereen alleen maar aan patiëntengegevens, maar medewerkersgegevens zijn natuurlijk net zo belangrijk.

RS: Nou dat is natuurlijk waar, die zijn net zo belangrijk.

Zorginstelling B: Ja en dat vind ik dus de valkuil hè, want we zijn als zorg heel erg gefocust op de patiëntengegevens en aan de ene kant is dat goed, maar aan de andere kant is dat bijna een uitnodiging om de medewerkersgegevens te verwaarlozen.

RS: Ja, ja dat kan ik me zo voorstellen. Want ik kan me bijvoorbeeld ook voorstellen dat artsen best een moeilijke groep zijn om hierin te bereiken. Heel zelfstandig werken ze natuurlijk. Ja op wat voor manier is er bijvoorbeeld gekeken hoeveel weten ze hier nu eigenlijk van? Doen ze hier iets mee?

Zorginstelling B: Nou daar is geen onderzoek naar gedaan. Uh, er wordt gecommuniceerd naar hen ook via het stafbestuur, dus zij worden ook gericht benaderd, maar bij alle communicatie is het zo dat je last hebt van een zender en een ontvanger, maar dat is niet alleen bij dokters zo.

RS: nee, dat is bij elke groep zo natuurlijk. Maar werden er bijvoorbeeld presentaties gegeven op afdelingen of was dat aan de afdelingen zelf om te bepalen?

Zorginstelling B: Uhm, dat gebeurt. Presentaties op afdelingen, maar artsen zijn geen onderdeel van de afdeling. Tenminste op de meeste plaatsen niet en op specifieke afdelingen wel natuurlijk, maar op de meeste plaatsen niet, dus die kun je op die manier niet bereiken.

RS: Oké en hoe kun je dat dan bijvoorbeeld wel doen?

Zorginstelling B: Via de staf. Zij hebben ook stafoverleg één keer in de zoveel tijd. Op die manier probeer je die dan te bereiken of via mailing, dat soort dingen.

RS: Ja en rondom die datalekken, wat zijn er dan bijvoorbeeld voor communicatiemiddelen geweest? Je noemde volgens mij al, het nieuwsblad dat elke week verschijnt, bijvoorbeeld ook nog iets van flyers of iets wat opgehangen werd?

Zorginstelling B: Nee, flyers niet. Er is aandacht besteed aan inderdaad de nieuwsbrief waarin ook verwezen werd naar ons intranet, waarin ook voorbeelden staan over waar je dan aan moet denken bij datalekken gewoon uit de dagelijkse praktijk in de zorg hè, als je op internet gaat zoeken vind je er genoeg. Dus op die manier besteed je daar aandacht aan, maar dan is, wat ik nou ga vertellen is meer verweven in mijn werk als

risicomanager en ik ben vorig jaar begonnen met risicomanagement en dan moet je ook jezelf presenteren en duidelijk maken waarom gaat het nu als je het hebt over risico's en dan komt informatiebeveiliging ook aan bod en dat heb ik gepresenteerd in iedere sector in het ziekenhuis.

RS: Oké dus dat was een beetje om de risico's onder de aandacht te brengen?

Zorginstelling B: Ja, maar dan besteed je dus impliciet ook aandacht aan informatiebeveiliging. Dat is daar een onderdeel van natuurlijk, dat is één van de facetten van de risico's die er zijn. Dus op die manier ben ik ook in alle sectoren geweest en dus ook bij de staf.

RS: Oké en wat zijn dan bijvoorbeeld voor jullie mogelijke gevolgen van zo'n data issue, privacy issue?

Zorginstelling B: Ja, ik denk dat dat bij ons is net zoals in ieder andere zorginstelling is. Er is heel veel aandacht voor natuurlijk de boetes die je kunt krijgen als je je datalekken niet meldt. Ik denk dat de risico's veel groter zijn op het vlak van imagoschade en dat soort dingen zeg maar. Dat zijn de belangrijkste risico's vind ik bij privacyschending.

RS: Ja, ligt er misschien ook een beetje aan hoe groot het issue is. Nou volgens mij heeft privacy in jullie organisatie al een redelijk hoge prioriteit in ieder geval, jullie zijn er al veel mee bezig en denk je ook dat medewerkers hier al echt bewustzijn voor hebben of hier mee bezig zijn?

Zorginstelling B: Ja, steeds meer, maar medewerkers bereiken is best lastig. Wat ik net al zei en dat geldt voor dokters en voor medewerkers je hebt bij iedere communicatie een zender en een ontvanger en dat is lastig, want die ontvanger heb je in feite geen invloed op. Als je iets niet wil horen, dan hoor je niks. Maar wat ik bijvoorbeeld ook doe is één keer in de maand lees ik logins uit.

RS: Leest u sorry?

Zorginstelling B: logins uit van ons EPD en dan ga ik gewoon gericht kijken van wie heeft er nu waar in gezeten en waarom en daar komen natuurlijk vragen uit voort en dat werkt heel erg goed.

RS: Oké en hoe gaat dat dan bijvoorbeeld in z'n werk? Je kunt dan gewoon in een bestand zien wat medewerkers in de afgelopen tijd…

Zorginstelling B: Ik kan alles zien wat medewerkers in de afgelopen tijd, wat iedereen doet in het EPD. In andere systemen is dat wat moeilijker, een aantal systemen kan dat wel, een aantal kan dat niet. Maar wat je dan doet is, om te beginnen kijk ik altijd, dan wordt het heel technisch hoor, maar als je in de EPD dan heb je vrij toegang tot een dossier als je daar een behandelrelatie mee hebt, dan wordt dat ook gelogd maar dan kun je er zomaar in. Op het moment dat je een dossier in wilt, waarvan niet in het EPD duidelijk is dat je daar een behandelrelatie mee hebt dan krijg je een pop-up van waarom wil je hierin? En dat noemen ze de break the glass methode. Daar staan een aantal voorkeuzes en de laatste is anders en dan moet je het zelf invullen hè als die keuze er niet in staat. Daar begin ik altijd mee om gewoon van een aantal weken te kijken, wie heeft de break the glass methode gebruikt en dan kijk je naar de redenen. Dan haal je er bijna altijd wel een paar uit waarvan je denkt ja wat staat hier nou eigenlijk want dan is het gewoon niet duidelijk dus dan krijgen mensen er een mail over van je hebt dat als reden opgegeven maar wat betekent dat nou?

RS: Ja, precies.

Zorginstelling B: Maar het komt ook voor dat mensen daar opgeven van nou dat doe ik omdat ik een eerste consult wil afspreken en dan ga je kijken, maar kan je geen eerste consult vinden. Nou, daar krijgen mensen ook een mail over. Ik zie dat je daar de reden opgegeven hebt: eerste consult, maar ik zie hem niet, wat is er aan de hand? Of je hebt een collegiaal consult of nou noem maar op.

RS: Ja.

Zorginstelling B: En dat werkt heel erg goed, want dat is natuurlijk geen officiële communicatie, maar wat er dan gebeurt is dat mensen onderling gaan praten van 'hee ik krijg een mail en ik moet verantwoording afleggen waarom ik dit of dat doe en dat spreekt zich heel snel rond'.

RS: Ja, dan gaan mensen er natuurlijk over nadenken van ik kan ook zo'n melding krijgen.

Zorginstelling B: Ja, ik krijg nu zelfs soms mailtjes van mensen die zeggen ja ik ben in dat dossier geweest en daar en daarom dan weet je dat vast.

RS: Ja, precies, alvast om zich te behoeden eigenlijk.

Zorginstelling B: Ja en dat is natuurlijk wat je wilt. Je wilt dat mensen erover na gaan denken van moet ik hier wel in?

RS: Ja, ja.

Zorginstelling B: En ik ga in principe uit van goede bedoelingen van iedereen en toch is het zo dat mensen soms, ja om een onbenullige reden in een dossier gaan kijken. En ja dat moeten we ze gewoon afleren.

RS: Ja, precies ja. Ik kan het me ook wel voorstellen inderdaad.

Zorginstelling B: Om je een voorbeeld te noemen, een recent voorbeeld. Krijg ik van iemand een mailtje, die voelde natuurlijk al wel dat dat niet deugde, maar die had een boek geleend van een patiënt en een beetje te lang in zijn bezit gehouden en die was dan in het EPD gaan kijken of die patiënt nog leefde, want die was ernstig ziek toen ze dat boek uitleende. Ja, ik snap het wel, maar het mag gewoon niet. Daar is het EPD niet voor bedoeld.

RS: Nee, dan moeten ze maar op een andere manier contact zoeken.

Zorginstelling B: Ja en dan vragen ze natuurlijk aan mij, hoe moet ik het dan doen. Ja, dat weet ik niet. Daar ben ik niet voor, maar het mag niet.

RS: Ja, dan maar opzoeken op Facebook.

Zorginstelling B: Ja, maar ja die oude baasjes die staan vaak niet op Facebook hè. Maar dat soort dingen die probeer je er natuurlijk uit te krijgen. Het is hartstikke goed bedoeld en dat geloof ik ook meteen, maar het mag gewoon niet. Dan moet je het op een andere manier oplossen. Nou dat soort dingen probeer je eruit te halen. En dan heb je natuurlijk ook en dat heb je in ieder ziekenhuis, dat je toch even gaat kijken waarom de buurvrouw in het ziekenhuis was. Ja, dat mag natuurlijk helemaal niet. Dan krijgen mensen ook echt een gesprek. Als je dat soort dingen signaleert van wat ben je nou aan het doen?

RS: En krijgen ze dan dat gesprek met jou?

Zorginstelling B: Ja. En met hun leidinggevende.

RS: Oké dus daar wordt ook wel op toegezien dat dat soort dingen…

Zorginstelling B: Ja, natuurlijk. Dat mag gewoon niet.

RS: Nee.

Zorginstelling B: En je kunt het niet altijd achterhalen, want je bent natuurlijk wel gebonden, ook ik moet me aan de privacyregels houden en wat ik bijvoorbeeld niet mag en eigenlijk wel graag zou willen is gewoon postcodes vergelijken. Postcodes van medewerkers en patiënten. Maar dat mag niet, want je hebt doelbinding.

Toch vind ik het wel jammer dat dat niet mag, want dan kun je veel gerichter gaan zoeken van wie doet er nou wat.

RS: Ja, precies. Dan kan je het koppelen natuurlijk of ze inderdaad naar de buurvrouw op zoek zijn.

Zorginstelling B: Ja, inderdaad. Nu moet ik daar bij toeval achter komen. Maar dan kun je gerichter zoeken, maar dat soort dingen mag niet en daar hou ik me dan ook aan, maar ik vind het wel eens jammer.

RS: Ja, snap ik. Het is misschien ook wel verleidelijk.

Zorginstelling B: Ja, maar mensen doen het ook vaak omdat ze het toch wel eng vinden om het aan iemand gewoon te vragen van hoe is het nou. Maar ja het mag gewoon niet. En je moet het ook niet willen hè. Ik probeer mensen ook altijd uit te leggen privacy is één het mag gewoon niet dus je doet het niet. Maar daarnaast vind ik ook oprecht je moet het niet willen weten. Als jij mijn buurvrouw bent, dan moet ik toch niet willen weten waarom jij in het ziekenhuis bent geweest. Dat moet ik aan jou vragen en als jij dat niet wil vertellen dan moet ik dat niet willen weten. Daardoor breng je jezelf ook in de problemen hè, want je krijgt hele rare verhoudingen daarmee. Ik werk natuurlijk al heel lang in een ziekenhuis en heb daar echt de raarste dingen van gezien. Daar moet je echt, daarmee breng je echt jezelf ook in de problemen. Even los nog van de privacy is het heel handig dat jij dingen weet van de ander waarvan de ander niet weet dat jij ze weet.

RS: Oké want er zijn nu dus wel steeds meer medewerkers die ook uit zichzelf komen van ik heb hier en hier in gekeken bijvoorbeeld.

Zorginstelling B: Ja en daar was dit en dit de reden van. En meestal is dat dan een reden die ook legitiem is hè, maar niet altijd en dan probeer je mensen daar ook wel duidelijk op te wijzen, waarom dat dan niet mag en wat ik dan natuurlijk ook wel doe daar heb ik wel een lijstje van zeg maar en dan toch nog een keer gericht kijken van hebben ze het niet toch nog gedaan daarna.

RS: Ja, nog een keer.

Zorginstelling B: Ja, kijk als je ze gewaarschuwd hebt dat het niet mag en ze doen het dan toch wordt het serieus.

RS: En, want dat is dus een manier die vrij goed werkt om…

Zorginstelling B: Ja, dat spreekt zich rond hè, dat past natuurlijk ook wel een beetje bij de omvang van deze instelling. Hier wordt natuurlijk toch wel een beetje gesproken van het dorp, zeg maar. Wij hebben natuurlijk niet een enorme instelling dus heel veel mensen kennen elkaar en dan werkt dat natuurlijk beter dan in een academische kliniek waar je mensen tegenkomt die je nog nooit gezien hebt.

RS: Dus dan gaan mensen erover praten, want ik vroeg me inderdaad ook af wat werkt wel om medewerkers in staat te stellen om aan de regels te voldoen, maar dit is dan dus een goede manier.

Zorginstelling B: Ja, dit werkt. Dit werkt beter dan één keer in de week in zo'n blaadje wat zetten, want dat leest toch echt niet iedereen hoor.

RS: En zijn er dan nog andere mogelijkheden waarvan je denkt dat die misschien wel zouden kunnen werken?

Zorginstelling B: Ja, kijk er staat nog van alles op mijn lijstje, want we hebben altijd te weinig tijd zeg maar. Maar wat je natuurlijk graag zou willen is ook binnen een afdeling, gewoon eens casussen bespreken van wat kom je nu tegen en hoe zou je dat nu anders kunnen doen.

RS: Ja, precies dat is natuurlijk een goede methode, want in hoeverre denk je dan dat communicatie bij zou kunnen dragen aan het inperken van de risico's binnen de instelling?

Zorginstelling B: Nou kijk ik vind de belangrijkste rol van communicatie is echt mensen bewust maken van dat er regels zijn, maar mensen helpen zich daaraan te houden daar speelt communicatie niet zo'n rol.

RS: Ja, dat is vooral natuurlijk toezicht houden op of de regels worden nageleefd.

Zorginstelling B: Ja, en ook duidelijk maken dat daar ook echt op toegezien wordt.

RS: Ja.

Zorginstelling B: Mensen moeten merken dat dat gebeurt. Dat is hetzelfde als iedereen weet dat je niet door rood mag rijden maar toch gebeurt het veel.

RS: Ja, omdat op genoeg plekken ook geen flitsapparaat staat zeg maar.

Zorginstelling B: Precies, zo werkt dat toch. En daarmee wil ik niet zeggen dat mensen hier net zoveel de regels schenden als dat mensen op straat door rood rijden, maar het gebeurt wel. Dat kan ook niet anders. Ik bedoel er werken hier 2000 mensen.

RS: Ja, dat heb je overal in elke instelling natuurlijk. En wordt er bijvoorbeeld ook de voortgang gevolgd? Zijn er meer mensen hier nu mee bezig of minder?

Zorginstelling B: Hoe bedoel je dat?

RS: Nou bijvoorbeeld nu is al gesignaleerd dat meer medewerkers terugkoppelen van goh ik heb hier in gekeken. Merk je bijvoorbeeld ook in de organisatie dat mensen er meer mee bezig zijn, meer over praten?

Zorginstelling B: Ja, er wordt wel meer over gesproken, maar dat heeft niet alleen te maken met wat ik doe, maar dat heeft ook mee te maken dat wij in november vorig jaar het EPD in gebruik genomen hebben en vanaf dat moment zeg maar hebben wij nog strikter gekeken wie kan nu waarin en waarom en moet dat nu wel zo blijven. Daar zijn instellingen wel strenger in gemaakt dan dat ze waren en als dat soort dingen veranderen dan wordt er over gesproken. En dan weten mensen weer beter hoe de regels nou in mekaar zitten, want daar is natuurlijk toch nog wel discussie over, dat hou je altijd van is dit nou wel of niet toegestaan dat een medewerker dit wel of niet mag en behoort hij nou wel of niet bij het behandelteam. Daar is wel altijd discussie over, want je hebt natuurlijk ook wel een soort grijs gebied daartussen. Maar zo'n verandering zeg maar dat helpt wel in de bewustwording.

RS: Ja, en krijg je dan bijvoorbeeld ook van afdelingen iets te horen bijvoorbeeld ze lopen ergens tegenaan? En op wat voor wijze worden dat soort barrières dan opgepakt?

Zorginstelling B: Daar ging net het gesprek over. Dat gaat dan heel expliciet ging over een OK die toegang wil hebben tot de radiologiebeelden en dan is de discussie is nou die OK-assistent onderdeel van het behandelteam van de patiënt. Dat is zeg maar de bepalende vraag of zo iemand dat mag, daar bij mag bij die beelden, dus heb je een doelbinding en daar kun je op allerlei manieren naar kijken en dat was net heel erg aan de hand. Dat is best een ingewikkelde vraag ook nog waar we nog niet uit zijn zeg maar.

RS: Nee, precies.

Zorginstelling B: Dus wat we dan doen meestal is de betrokkene horen hè wat is nou jouw reden om dat wel te vinden of niet te vinden en dan bespreken we dat, bespreek ik dat meestal met de jurist en als we dat dan nog moeilijk vinden dan hebben we ook nog een autorisatiecommissie, dus dat is dan nog een wat groter verband waarin je dan discussieert.

RS: En bijvoorbeeld meer gericht op de medewerkers: mensen kunnen natuurlijk dingen mee naar huis nemen of mensen kunnen hun computer vergeten uit te loggen, wordt daar aandacht aan besteed?

Zorginstelling B: Ja, zeker daar wordt zeker aandacht aan besteed. Maar ja dat blijft tegelijkertijd ook wel een lastige.

RS: Ja, dat kan ik me voorstellen. Ik vind het zelf ook, je neemt heel snel dingen mee naar huis of je zet het op een usb-stick.

Zorginstelling B: Ja, ik vind dat enorm moeilijk. Hoe dicht je dat soort gaten nou af. En we hebben nog niet zo lang een incident daarmee gehad. Dat was een usb-stick die was vijf jaar geleden gemaakt en toen nog heel begrijpelijk want er moesten gegevens naar de zorgverzekeraar. Dat kon niet anders in die tijd als met die usb-stick. Maar zo'n usb-stick die ligt nog in zo'n la en op een gegeven moment zo'n la van zo'n ladeblok en die is stuk en die wordt afgevoerd en dan vinden we die usb terug. Nou gelukkig vinden wij hem op dit terrein nog terug, maar voor hetzelfde geld.

RS: Ja, dat is dan mazzel.

Zorginstelling B: Ja, voor hetzelfde geld. En ja dat is wel ingewikkeld.

RS: Ja, en merk je dan bijvoorbeeld ook een verandering sinds de Wet Meldplicht Datalekken is ingegaan?

Zorginstelling B: Ja, je probeert mensen daar meer en meer bewust van te maken en dat lukt ook wel, maar daarmee maak je het niet waterproof zeg maar.

RS: Nee, nee, dat is zo.

Zorginstelling B: Dat is ook bijna niet mogelijk denk ik.

RS: Want zijn er bijvoorbeeld al dingen in het beleid van hoe bijvoorbeeld je een melding doet van een datalek?

Zorginstelling B: Ja, ja zeker. Ja, daar is een procedure voor, want er is natuurlijk ook een procedure voor wat je wel en niet op lokale media mag opslaan, maar daar is ook beleid voor. Hoe ga je om met verwisselbare media. En het is ook zo dat in principe hier de usb-uitgangen niet werken, dus alleen op aanvraag en op argumentatie wordt die open gezet, maar daarmee maak je het niet waterproof. Nog steeds niet.

RS: Nee, mensen kunnen het ook naar hun laptop sturen op één of andere manier via Gmail kan natuurlijk ook van alles misgaan. En hebben jullie dan bijvoorbeeld een intern meldpunt waar medewerkers melding kunnen doen?

Zorginstelling B: Ja, wat we gedaan hebben in onze VIM-applicatie, ik weet niet of je dat wat zegt? VIM is een systeem Veilig Incident Melden daarmee kun je dus meldingen maken over incidenten daar hebben wij een categorie gemaakt informatiebeveiliging en dan kunnen ze dat invullen dan krijg ik daar samen met de andere twee leden van de informatiebeveiligingscommissie een mail van. En daarop ga ik dus aan de slag van wat is er nou precies gebeurd en moet dit gemeld worden en hoe dichten we het lek en noem maar op, dus ja.

RS: En wordt de medewerker daar dan ook in meegenomen?

Zorginstelling B: Die krijgt terugrapportage en heel vaak, maar dat is niet altijd nodig, benader ik die dan ook van ja hoe zit dit en hoe zit dat.

RS: Ja, want je hebt natuurlijk dat formulier op internet dat je moet invullen van de Autoriteit Persoonsgegevens, die is vrij uitgebreid. Je hebt dan natuurlijk 72 uur om het te melden.

Zorginstelling B: Die 72 uur als ik er ben is dat oplosbaar.

RS: Ja, nee dat is zeker waar. Maar bijvoorbeeld weekenden is natuurlijk ook een punt.

Zorginstelling B: Nee ik ben er in het weekend niet, maar daar is die 72 uur voor. Het zou eerst 48 uur worden, maar dan heb je in de weekenden een probleem, maar wij hebben het zo geregeld dat met ons drieën er is altijd iemand. Dus als ik vakantie neem dan neemt één van die andere twee dat over.

RS: Oké ja, want inderdaad je hebt natuurlijk in zorginstellingen als je denkt aan crisiscommunicatie, een communicatieteam staat eigenlijk altijd offline bereikbaar voor mocht er wel iets gebeuren. Is er hier in het ziekenhuis zijn er wel dingen geregeld van mocht er nou iets ernstigs gebeuren bijvoorbeeld in het weekend dat dingen geblokkeerd kunnen worden? Bijvoorbeeld als iemand in de trein zit met een laptop en die wordt gestolen of iets dergelijks dat dat soort dingen geblokkeerd kunnen worden meteen?

Zorginstelling B: Als een laptop gestolen wordt kun je er niet bij.

RS: Ja, dat ligt eraan wat voor laptop het is natuurlijk, als die van het ziekenhuis is.

Zorginstelling B: Ik denk van niet, maar in principe is het zo dat als mensen in het ziekenhuissysteem willen dan moeten zij hun account openen. En dat kunnen we stoppen. En er is een dienstdoende van de ICT, dus ja dat kan.

RS: Oké dus het is wel zo dat het in ieder geval niet erger kan worden.

Zorginstelling B: Maar hebben mensen lokaal wat staan en het wordt gestolen, dan kun je niet verder. Daar kun je niet bij dat kun je niet blokkeren van afstand.

RS: Nee, als mensen lokaal dingen hebben opgeslagen niet, nee.

Zorginstelling B: Maar het beleid is dat ze dat niet mogen doen.

RS: Dat is natuurlijk zo. Het beleid is natuurlijk bijvoorbeeld bij het Antoni van Leeuwenziekenhuis waren toen heel veel dossiers gestolen uit iemands auto, die had het mee naar huis genomen, maar die ging nog even wat drinken ergens.

Zorginstelling B: Ja, dat zijn van die voorbeelden waarvan iedereen weet dat dat niet mag, maar toch gebeurt het. En daar durf ik hier mijn hand ook niet voor in het vuur te steken. Er wordt genoeg over gecommuniceerd en mensen weten intussen wel dat dat niet mag.

RS: En weten ze ook dat ze dat meldpunt hebben? Is daar ook over gecommuniceerd dat ze dat kunnen gebruiken?

Zorginstelling B: Ja, zeker.

RS: En ze weten ook hoe dat moet?

Zorginstelling B: Ja, dat moeten ze weten, want ze moeten ook andere incidenten daarop melden.

RS: Ja, je hebt natuurlijk ook kwaliteitsincidenten. Want zijn er dan bijvoorbeeld extra communicatiemiddelen ingezet na de Meldplicht Datalekken dat die is ingevoerd?

Zorginstelling B: Ja wij hebben gecommuniceerd over die wet, dat die er is en hoe ze datalekken moeten melden en dat soort dingen dat gaat overigens op dezelfde manier als ieder ander veiligheidsincident, maar dat hebben we wel weer opnieuw gecommuniceerd ja.

RS: Ja, en dat gaat dan via die applicatie of via het computerscherm kun je die meldingen doen?

Zorginstelling B: Ja dat kan via intranet hè, kun je die melding doen.

RS: En heb je ook bijvoorbeeld een telefoonnummer of iets dergelijks dat je kunt bellen bij dit soort zaken?

Zorginstelling B: Ja, als ik heel eerlijk ben.

RS: Als je bijvoorbeeld in de trein zit en je hebt een usb-stick of iets wat je kwijtraakt.

Zorginstelling B: Ja, mijn nummer dat heb jij ook gevonden waarschijnlijk, dat staat gewoon op internet.

RS: Ja, klopt. Ja, want internet noem je nu en voor externen, want je hebt natuurlijk ook mensen die met goede bedoelingen in je systeem gaan kijken van lekken hier dingen of staan hier ergens dingen die hier niet horen? Hebben jullie daar een meldpunt voor?

Zorginstelling B: Dat is hetzelfde meldpunt hè.

RS: Oké dus dat is hetzelfde als het interne meldpunt?

Zorginstelling B: Ja, alleen vanuit extern kun je natuurlijk niet bij die VIM-applicatie, maar als je gaat kijken naar het internet dan staat ook bij privacy staat dat als ze daar klachten of vragen over hebben dat ze mij kunnen bellen.

RS: Ja, precies. Dus op die manier wel. Want ik heb volgens mij ook wel eens bij een website gezien van een gemeente bijvoorbeeld dat er zo rechts in de hoek staat van: 'meld uw datalek'.

Zorginstelling B: Ja, zo staat dat er bij ons niet. Maar wel als je privacy intypt op de zoeker dan kom je bij mij terecht.

RS: Ja, precies. En wat voor dingen denk je dat mensen gaan motiveren om te gaan melden bijvoorbeeld? Want ik kan me voorstellen dat je ook wel eens denkt van ik weet niet of ik dit wel wil melden?

Zorginstelling B: Ja, maar kijk je kunt niet meer doen dan mensen erop wijzen dat het belangrijk is om te melden en waarom het belangrijk is. Over het algemeen is het toch gewoon zo dat medewerkers in de zorg het ook wel belangrijk vinden dat privacy bewaakt blijft dus ze hebben ook wel een interne motivatie, ja en er is dan die VIM-melding waarbij het juist nadrukkelijk bedoeld is om mensen zonder dat daar represailles tegenover staan ook kunnen melden. Ja veel meer kun je niet doen.

RS: Kunnen ze bijvoorbeeld anoniem melden of melden ze wel bij naam altijd?

Zorginstelling B: Ik denk, maar dat weet ik niet zeker, dat je je naam niet perse in hoeft te vullen.

RS: Dat is voor jou natuurlijk wel handig als ze dat wel doen, want anders weet je ook niet…

Zorginstelling B: Nee, dan weet ik ook niet waar ik moet zoeken.

RS: Precies.

Zorginstelling B: Maar ik heb het ook nog nooit meegemaakt dat er een naam niet bijstond zeg maar.

RS: En je hebt natuurlijk die melding, die gaat dan naar de Autoriteit Persoonsgegevens hebben jullie daar ook dingen van gekregen? Informatie vanuit hen?

Zorginstelling B: De algemene communicatie die iedere zorginstelling heeft gehad.

RS: Ja, oké dus gewoon, maar wel naar jullie gericht of gewoon wat op de website te vinden is?

Zorginstelling B: Ja, nee je krijgt ook gerichte communicatie.

RS: Oké.

Zorginstelling B: Ook via de NVZ hè.

RS: En bijvoorbeeld hoe kijk je dan tegen de rol aan van de Autoriteit Persoonsgegevens in dit verhaal?

Zorginstelling B: Tsja… Ik moet zeggen dat ik niet vind dat die heel proactief zijn.

RS: Nee, ja want als je bijvoorbeeld ik kan me voorstellen dat je soms een datalek hebt of een mogelijk lekt hebt en je hebt daar vragen over dan zou je denken goh dan bel ik de Autoriteit Persoonsgegevens op.

Zorginstelling B: Ja, dat kan hè. Er is een telefonisch spreekuur iedere dag.

RS: Ja, maar zou dat een mogelijkheid zijn om dat te doen?

Zorginstelling B: Ik heb wel eens met hen gepraat.

RS: Oké en kreeg je dan ook antwoord op je vragen?

Zorginstelling B: Ja, uiteindelijk wel, ja ik vind wel, ja je krijgt wel antwoord op je vragen, niet altijd een bevredigend antwoord maar goed dat ligt niet alleen aan hen maar ook aan mij denk ik, maar wat wel lastig is je belt dan naar zo'n telefonisch spreekuur dan heb je niet altijd degene ervoor die jouw antwoord kan geven, dus soms gaat er dan toch wel wat tijd overheen voor je antwoord hebt. Uiteindelijk krijg je het wel is mijn ervaring, maar soms duurt het wel te lang.

RS: Ja en want je kreeg natuurlijk die Wet Meldplicht Datalekken, dus Wet Bescherming Persoonsgegevens al die artikelen en dergelijke. Was dat duidelijk allemaal?

Zorginstelling B: Niet altijd natuurlijk maar weet je we hebben hier een regionale privacycommissie waarbinnen we ook over dit soort dingen spreken. Ik zit in het netwerk informatiebeveiliging dus je krijgt ook via het netwerk krijg je informatie, dus uiteindelijk kom je daar wel uit.

RS: Ja, dat is zo natuurlijk. Ik ben toevallig ook naar een bijeenkomst geweest van de NVFG toen was er ook iemand van de Autoriteit Persoonsgegevens aanwezig, Udo Oelen geloof ik. Die probeerde wel echt wat meer benaderbaar en toegankelijk te zijn, maar ik merkte toch wel heel veel afstand van de mensen die in de zaal zaten, als in niet durven zeggen van welke instelling je komt.

Zorginstelling B: Ja, maar iedereen is er bang van hè. Ja, en misschien wel terecht ik weet het niet kijk tot nu toe is er natuurlijk nog niets gebeurd en dat was natuurlijk ook wel de verwachting het was niet te verwachten dat per 1 januari meteen de boetes om de oren zouden vliegen.

RS: Nee, daar hebben ze de capaciteit ook niet voor.

Zorginstelling B: ook dat nog, maar het zou ook contraproductief zijn, want dan zouden mensen ook schroom gaan krijgen om dingen te melden, dus dat was ook niet te verwachten. Maar uiteindelijk zullen zij natuurlijk gaan handhaven en ook wel terecht, maar je zou een gemakkelijkere toegang tot hen moeten hebben en tot hun kennis moeten hebben. Maar ik denk dat wat jij zegt daar hebben zij uiteindelijk ook helemaal de capaciteit niet voor.

RS: Nee, daar zouden zij eigenlijk wel meer capaciteit voor mogen krijgen. Want dit is natuurlijk een soort tussenperiode: je hebt tot één januari 2018 dan heb je de AVG. In hoeverre denk je dat jullie daarop voorbereid zijn tegen die tijd?

Zorginstelling B: Nog niet. Er zijn echt nog dingen die anders moeten en zoals ik al zei we zitten in zo'n regionale privacycommissie, dus dan ben je ook wel op zoek zeg maar om daar wat in de gezamenlijkheid aandacht aan te besteden om het wel op tijd op orde te krijgen.

RS: Ja, want is daar een stappenplan voor bij jullie?

Zorginstelling B: nog niet.

RS: Oké.

Zorginstelling B: Dat moet er wel komen natuurlijk, maar dat is er nog niet.

RS: Ja, in een onderzoek van Dell wat ik heb gezien zeiden ze dat 97% van de bedrijven eigenlijk nog geen plan heeft voor die verordening, waar denk je dat dat door komt?

Zorginstelling B: Het duurt nog lang natuurlijk hè.

RS: Ja, dat is zo. In principe heb je nu natuurlijk de Wet Meldplicht Datalekken en dat verandert niet zo heel veel bij die Europese Verordening, tenminste dat heb ik begrepen op congressen waar ik aanwezig ben geweest en zelf ook even in heb verdiept.

Zorginstelling B: Ja wat betreft de Meldplicht wel maar er zijn natuurlijk dingen die net iets anders moeten al gaat het alleen maar om toestemming over het uitwisselen van gegevens daar wordt de regelgeving strikter.

RS: Bewerkersovereenkomsten dat soort zaken.

Zorginstelling B: Bewerkersovereenkomsten die zijn er natuurlijk nu ook al, maar dat wordt wat strikter. Dus daar moeten we nog wel mee aan de slag, ik heb nog geen plan.

RS: Nog wel ideeën daarover?

Zorginstelling B: Nou dat moet gaan komen, ja dat moet zeker gaan komen, maar zoals ik al zei proberen we het toch een beetje regionaal op te pakken zodat we niet allemaal zelf het wiel aan het uitvinden zijn.

RS: Nee, precies dat is een hele goede denk ik ook, want er zal natuurlijk niet altijd evenveel budget voor zijn om dingen door te voeren.

Zorginstelling B: Nee, niet en de tijd ontbreekt soms ook he.

RS: Ja, daarom. Zeker als ik zo hoor dat het nog geen fulltime functie is.

Zorginstelling B: Ja, maar dat gaat het in deze instelling ook niet worden. Dat is onbetaalbaar. Kijk dat is het lastige hè met een instelling van onze omgang. Je kunt niet voor al dit soort dingen iemand aanstellen, want dat is veel te duur.

RS: Ja, precies, dus dan is het ook inderdaad handig om die regionale samenwerking op te stellen. Je kan natuurlijk wel een externe FG delen met meerdere instellingen.

Zorginstelling B: Ja, snap ik, ook dat kost vaak een hele hoop geld.

RS: Nou ik denk dat ik heel veel informatie heb gekregen dus dat is in ieder geval een goed teken. Ik zit nog even te kijken of ik alle vragen heb behandeld, het is natuurlijk belangrijk dat ik bij elke zorginstelling een beetje dezelfde vragen stel. Volgens mij heb ik alles.

Nog belangrijke quote uit nagesprek:

'Je moet niet eenmalig iets met communicatie doen, want dan verliest het focus'.

5.3 Uitwerking Interview zorginstelling C

RS: De functie is natuurlijk vrij nieuw de functie van privacy officer, functionaris gegevensbescherming dus ik was benieuwd: hoe ben je op deze plek terechtgekomen, bij deze functie?

Zorginstelling C: Nou ik werk al sinds 2003 bij deze instelling. Ik ben begonnen bij een secretaressefunctie eerst bij de jeugd gezondheidszorg en in 2008 ben ik doorgestroomd naar de Raad van Bestuur. Eind vorig jaar kwam de functie functionaris gegevensbescherming op de borden hier en toen werd ik benaderd door onze bestuurder of ik daar interesse voor zou hebben. Daar heb ik even, nou ja best even over nagedacht, want het is natuurlijk een hele andere soortige functie en ik heb ook helemaal geen juridische achtergrond ik heb ook helemaal geen ICT-achtergrond dus ja, ik moest eigenlijk in het diepe gegooid worden. Ik ben uiteindelijk wel de selectieprocedure ingegaan en ben toen per 1 december aangesteld als FG-er. Ik doe de functie wel met ondersteuning van de informatiemanager, dus ik doe het niet helemaal alleen. Ik heb wel een onafhankelijke positie, maar op ICT-gebied word ik echt ondersteund door de informatiemanager en hij is ook vorig jaar al betrokken geweest bij onder andere de risico-inventarisatie. Dus hij is vanaf het begin af aan eigenlijk betrokken geweest bij het hele traject.

RS: Is het een fulltime functie of parttime?

Zorginstelling C: Nee, ik werk 16 tot 24 uur, doe ik de functie en ik weet natuurlijk niet hoeveel uren de informatiemanager er exact aan besteed, maar het zal om en nabij in zijn totaliteit om een fulltime functie gaan. Ja, we zijn natuurlijk een zorginstelling dus we werken veel met gegevensverwerkingen, dus er komen ook veel vraagstukken naar voren en ik moet wel eerlijk zeggen dat ik een tijd in een overgangsfase heb gezeten. Mijn collega kreeg ook een andere functie hier intern en onze oude functie die werd niet gelijk naar behoren ingevuld dus we hebben een tijd met één been hier en één been daar, maar goed sinds 1 september is het echt goed gefaciliteerd en kan ik mij echt helemaal richten op deze functie.

RS: En hoe zit dit dan in de organisatie verworven zeg maar? Valt dit onder een speciale afdeling of?

Zorginstelling C: Nee, nog niet. Wij zijn wel momenteel aan het kijken naar een andere organisatiestructuur waarbij mijn functie waarschijnlijk wordt ingedeeld bij afdeling beleid, zo'n functie komt er weer en ik denk ook dat de positie daar goed zit. Ik hang nu echt onder de Raad van
Bestuur en dan kom ik onder een concernmanager. Zo ziet het plaatje eruit, maar we hebben geen aparte afdeling privacy of security. We zijn ook maar met zijn tweeën.

RS: Nee, dat zie je op dit moment nog wel veel vaker hoor. Het is natuurlijk een heel actueel thema, maar het is nog vrij in het beginstadium. Vandaar ook dit praktijkonderzoek om echt even te kijken waar staan we nu in het veld en wat kunnen we hieraan bijdragen.

Zorginstelling C: Nou wij hebben zeg maar wel een stuurgroep, een stuurgroep informatiebeveiliging, daar zit de bestuurder ook bij, de informatiemanager en ik zitten daarbij. En we hebben een klankbordgroep die komen eens per kwartaal bij elkaar, de stuurgroep maandelijks en we hebben altijd maandelijks MT waar dit punt ook wel op de agenda staat. Dus het is in die zin wel geborgd overal, maar wij zitten momenteel best in een periode waar andere zaken ook hoge prioriteit hebben en dan merk je toch dat, tenminste dat idee heb ik, dat het bij mensen is van oh heb je dat gezeur weer, moeten we dat ook weer gaan doen. Dus dat is best een beetje lastig.

RS: Want je hebt natuurlijk functionaris gegevensbescherming en je hebt privacy. Hoe staan die twee tot elkaar in verhouding?

Zorginstelling C: Ja, bij ons is dat allemaal één pot nat zeg maar.

RS: Dus eigenlijk je houdt je niet alleen bezig met de bescherming van de persoonsgegevens maar ook met privacythema's, die vallen ook onder jou.

Zorginstelling C: Ja, we hebben daar geen scheiding in. Nee, alles valt onder één en dezelfde noemer.

RS: Ja, nee precies. Want hoe groot is deze instelling ongeveer? Hoeveel mensen werken hier?

Zorginstelling C: uhm, om en nabij de 2000.

RS: Oh behoorlijk wat.

Zorginstelling C: Ja, we zijn al fors ingekrompen maar er zijn nu nog ongeveer 2000 medewerkers.

RS: Oké en als er dan bijvoorbeeld beleid wordt opgesteld rondom dit thema ben jij dan degene die dat aankaart?

Zorginstelling C: Ja, in combinatie. Wij hadden geen Sec of privacybeleid, dus daar zijn we vorig jaar mee aan de gang gegaan. Daar heeft de informatiemanager als eerste het voortouw in genomen. Dus hij heeft het beleid geschreven, want hij is tevens MT-lid. Ik heb op basis daarvan een informatiebeveiligingsplan geschreven en een plan van aanpak Meldplicht Datalekken dus met die drie notities hebben we zeg maar één grote notitie gemaakt en die is begin van dit jaar ook in het MT vastgesteld en die wordt nu geïmplementeerd in de organisatie verder.

RS: Oké, ja en ja wat voor soort beleid moet ik dan aan denken? Is dat bijvoorbeeld een privacyreglement?

Zorginstelling C: Ja, dat is onderdeel ervan. Nou we hebben die risico-inventarisatie uitgevoerd waar een aantal risico's naar voren kwamen die zijn onder andere daar benoemd, want ja hoe willen we met die risico's omgaan daar moeten wij als instelling wat van gaan vinden. We merkten dat er eigenlijk ook wel behoefte was aan een algemene gedragscode. We hebben heel veel losse dingen ICT, huisregels, gedragsregels eigenlijk miste daar wat: een algeheel beeld, dus daar zijn we mee aan de gang en ja bewustwording bij de medewerkers dat is bij ons wel een heel groot punt waar we mee bezig gaan. We hebben bij onze ICT-omgeving, zijn we vorig jaar overgegaan naar een platform, dat is helemaal beveiligd, dus die beveiliging zit wel goed, maar ja hoe ga je nou om bij de medewerkers of hoe gaan de medewerkers om met gebruik van Whatsapp en Social Media. Nou daar hebben we niks over.

RS: Ja, ja precies, want wat voor soort medewerkers zitten hier allemaal? Wat voor mensen hebben toegang tot bijvoorbeeld patiëntgegevens?

Zorginstelling C: Nou die zijn allemaal wel, we werken met een ECD, die is nu de pilotfase voorbij, dus die zijn we nu gefaseerd aan het invoeren. Ja, hier op kantoor werken voornamelijk beleidsmedewerkers er zit een stuk huishoudelijke verzorging, maar dat zijn dan de managers, de planners, de reïntegratiespecialisten op kantoor en de uitvoerende medewerkers dat zijn onder andere de wijkverpleegkundigen, huishoudelijke hulpen, maar ook artsen van de JGZ, verpleegkundigen van de JGZ, we hebben een heel breed scala van mensen die daar werken en die zijn allemaal op basis van hun functie, hebben die autorisatie gekregen voor wij werken met ONS van NEDAP dat is een cliëntendossier, een systeem en die zijn op basis van hun functie zijn zij geautoriseerd en hebben zij toegang.

RS: Oké en hoe benader je dan die groepen als je dat beleid hebt? Is daar een verschillende manier voor of wordt dat algemeen gedaan?

Zorginstelling C: Nee, daar zijn we aan het kijken. In eerste instantie is het zo dat het vanuit de top gaat. Het MT heeft die stukken vastgesteld, dan gaan die stukken via het betreffende MT-lid verder naar de divisie naar de leidinggevenden en de leidinggevenden die nemen dat dan weer mee in hun overleggen met de teams.

RS: Oké

Zorginstelling C: Het wordt gepubliceerd op intranet. Er wordt ook aandacht gegeven dat het gepubliceerd is dat het er staat. Maar daar heeft niet iedereen toegang tot want niet alle medewerkers hier hebben een eigen account. Want ja de gewone verzorgende die hoeft eigenlijk niks met een mailadres van de instelling. Dus ook op basis van kosten hoor is er voor gekozen om die geen account meer te geven. Dus die bereik je dan ook niet, zij hebben ook geen werkoverleggen, komen nauwelijks meer op kantoor, dus ja dat is lastig. Dat is een lastige groep om te bereiken.

RS: Ja, zijn daar ideeën over, hoe die groep te benaderen?

Zorginstelling C: Uhm, ja we hebben nu binnenkort hebben we een training privacy die wordt gegeven door een advocatenkantoor. Daar zit ook de leidinggevende van de HV (Hoofd Verpleegkundigen) bij en zij communiceren ja, via weer het ons medewerkersportaal, dus dan gaat het via die weg, hebben zij wel toegang.

RS: Oké dus ze gaan bijvoorbeeld ze worden in overleggen meegenomen de nieuwe regels en dergelijke en zijn er bijvoorbeeld ook nieuwsbrieven of andere vormen van communicatie?

Zorginstelling C: Ja, nieuwsbrieven gaan maandelijks, die verstuur ik. Die gaan ook wel weer via het intranet, maar ook deels via de mail. Met het verzoek ook om die breder te verspreiden. We gaan binnenkort een enquête uitdoen, een enquête gebaseerd op de NEN7510 die willen we een beetje als nulmeting gaan gebruiken van hè hoe leeft het nou bij de mensen en die willen we ook uit gaan zetten onder een breed scala dus zowel op topniveau als ook op het niveau van de werkvloer, maar ook bij de huishoudelijk verzorgenden en dan willen we hem over een half jaar of negen maanden weer een keer herhalen van wat is nu: hè hoe staat het nu is er wat veranderd en waar hebben mensen behoefte aan? Hoe zouden zij informatie graag aangedragen krijgen?

RS: Ja, oké en dat is dan meer algemeen? Meer om in beeld te krijgen hoe zouden mensen informatie tot zich willen nemen?

Zorginstelling C: Ja.

RS: En dan kan je daar natuurlijk weer op inspelen, want hebben jullie hier ook een communicatieafdeling?

Zorginstelling C: Ja.

RS: En sta jij daar aan verbonden als je bijvoorbeeld iets met communicatie wilt?

Zorginstelling C: Ja, als ik iets heb dan kan ik met hen contact opnemen. Toevallig, dus daarom kwam dit ook wel mooi uit, was er vanuit het MT de behoefte van goh schrijf nou eens op een A4tje wat belangrijkste speerpunten. Nou daar ben ik mee begonnen, maar met een A4tje kom je niet weg dus dat waren inmiddels drie A4tjes geworden, maar wel punten die ik wel van belang acht en ook gewoon dingen waar mensen thuis mee in aanraking komen hè. Dus toen zeiden ze van he goh misschien moet je eens met communicatie gaan praten en dat is een vrouw die is van extern aangetrokken, we hebben wel een interne communicatie maar die doen meer marketing.

RS: Oké ja dit is natuurlijk meer

Zorginstelling C: Ja iemand voor de PR ook meer aangetrokken. En zij zei ja je zou het kunnen doen met een puzzel van 1000 stukjes beneden neerleggen en dan ontbreken er twee stukjes of nou ja wat meer met een ludieke actie, met wuppies of nou ja ik noem maar wat dat je een wuppie informatiebeveiliging hebt, maar ik ken onze organisatie een beetje en ik weet dat dat in onze organisatie niet echt gaat werken. Ik denk dat als ik daarmee bij het MT aan kom.

RS: Nee, het zijn ook wel wat extreme ideeën.

Zorginstelling C: Ja, dat ze me heel hard uitlachen dus ik zei ik weet niet of ik dat wat vind.

RS: Ja, nee. Ja wij werken zelf dan ook veel samen met overheden en ook zorginstellingen, maar ja je moet natuurlijk wel altijd een beetje in kaart brengen eerst wat voor organisatie hebben we mee te maken? En hoe worden dingen normaal gesproken aangepakt als er iets nieuws aandacht moet krijgen in de organisatie. Binnen die kaders kun je vaak wel dingen aanpassen, maar als je iets heel nieuws gaat doen, komt het misschien ook wel rauw op mensen hun dak.

Zorginstelling C: Ja, en wij zijn er als organisatie niet heel sterk in hoor om dingen te communiceren. Wij mogen bij onze communicatie, dat komt overal naar voren bij de medewerkersmonitor, communicatie komt altijd naar voren als toch een zwak punt.

RS: Ja, is ook misschien wel een lastig punt. Zeker met zoveel verschillende afdelingen en verschillende soorten medewerkers, ja hoe bereik je al die groepen, dat is altijd lastig natuurlijk. Want hebben jullie toevallig ook meegedaan met de 'ZEKER' campagne, die is van de NVZ uit.

Zorginstelling C: Nee, maar toevallig was dat ook van zeker? Las ik vandaag wat, dat ze een mail hadden gestuurd aan 68.000 medewerkers over 28 verschillende ziekenhuizen over die taart, dat ze een taart konden winnen voor een beste zorgteam of de beste zorgmedewerker en dat was dan een fishingmail en dat kon je aan dat mailadres van de afzenders zien en zij brachten dus in kaart hoeveel mensen daarop klikken en op welk niveau wordt er nou toch op die link geklikt. Dus ik heb hem toevallig heb ik hem uitgeprint, en dacht ik die moet ik wel even meenemen want dat vond ik dus wel een hele ludieke manier van bewustwording van ja waar klik ik nou eigenlijk op.

RS: Nee, ja precies. Dat is ook iets waar mensen niet snel over nadenken. Men denkt van oh leuk een taart, ik kan wat winnen.

Zorginstelling C: nee, maar ik heb niet was dat van zeker?

RS: Nou de 'ZEKER' campagne was ook om informatiebeveiliging onder de aandacht te brengen van medewerkers, daar hebben iets van 80 zorginstellingen aan meegedaan, liep in oktober. Dus je kunt nog steeds de test en alles vinden voor medewerkers.

Zorginstelling C: Ja die heb ik volgens mij wel, maar dat was volgens mij wel specifiek voor ziekenhuizen of niet?

RS: Nee, voor verschillende soorten zorginstellingen, maar daarin ja wat daarin eigenlijk vooral werd gedaan was meer alert maken, bijvoorbeeld een quizje online. En ik was heel erg verbaasd want ik zag de uitslag en er stond dat 97 procent van de medewerkers was voorbereid of ging goed om met informatiebeveiliging, dus ik vond dat een beetje vreemd. Dus ik dacht ik ga eens even verder kijken, maar ja inderdaad voor het aandacht geven voor het thema is het iets moois, maar de uitslag klopte niet echt.

Zorginstelling C: Ja, en volgens mij heb ik hem zelf ook gedaan. Het komt me wel heel bekend voor.

RS: Nou er was één vraag die vond ik nog wel lastig met die dossiers die je moest invullen. Voor de rest waren het vragen als: een medewerker loopt weg bij een computer wat doe je? En dan kon je uit MPC-antwoorden kiezen.

Zorginstelling C: Ik denk ook dat die gekoppeld was aan Alert Online he?

RS: Ja klopt, maar vanuit zoiets zit er natuurlijk altijd een gedachte achter. Maar hebben jullie dan andere soort campagnes om medewerkers alert te maken?

Zorginstelling C: Nou we hebben nu wel ook aangehaakt op Alert Online, was voor ons ook het eerste jaar dat wij daaraan meededen. Wij hebben toen wel de quiz die zij online ook beschikbaar hebben gesteld die hebben

wij ook op ons intranet beschikbaar gesteld voor de medewerkers. We hebben iedere dag bij het inloggen een leus of een tekst kort over informatieveiligheid en dan iedere keer een ander onderwerp met een plaatje erbij.

RS: Oké dat komt dan in het scherm waar je moet inloggen zeg maar?

Zorginstelling C: Ja, dat hebben we aan die campagneweek opgehangen. En het idee is nu dat is ook van die externe communicatiedame waarvan ik dacht ja dat vind ik wel een goede om een digitaal poppetje te creëren en die af en toe over je scherm te laten komen met een kreet. Weet je dat is niet dat bij iedereen meteen de alarmbellen gaan rinkelen, maar wel dat het iets is wat mensen bij blijft en wel dat dat poppetje dan gekoppeld is aan informatiebeveiliging, dus dat dat gewoon één gezicht gaat worden. Daar kon ik me wel in vinden, ik dacht dat vind ik wel een leuk iets tastbaars waar je wat mee zou kunnen.

RS: Oké en dat zou dan voor alle medewerkers op het scherm…

Zorginstelling C: Ja, maar je zit dan altijd weer met die groep die dan geen scherm heeft.

RS: Ja, want je hebt hier dan vaste computers en daar kun je dat dan op instellen of ook?

Zorginstelling C: Ja, ik weet niet hoe dat ICT-technisch zou moeten, maar goed dat zou kunnen. Op laptops zou dat ook moeten kunnen, want wij werken via dat platform en dat kan overal inloggen op je tablet of op je laptop of op je telefoon dus daar zou dat dan denk ik overal op alle devices wel moeten kunnen.

RS: En worden er ook bijvoorbeeld maatregelen getroffen als medewerkers een gedragscode of regel niet naleven?

Zorginstelling C: Uhm, nog niet, omdat we daar dus nog geen duidelijk beleid over hebben. Toevallig heb ik donderdag daar een afspraak over, daar willen we wel sancties aan gaan ophangen, maar wat voor sancties dat is nog een beetje onduidelijk. Maar daar zijn we wel mee bezig.

RS: Want je vertelde net ook van die enquête, dat is dan een soort nulmeting. Dus dat is ook een eerste soort van evaluatie van waar staan we nu? Dus dat wordt nu nog niet tussentijds geëvalueerd? Of dat je terugkoppeling krijgt van medewerkers?

Zorginstelling C: Nee, weet je wat het lastige is, wij hebben eind januari een informatiebijeenkomst gehouden, dat was voor het MT-team leidinggevenden hier en de ICT-afdeling, P&O, beleid. Daar waren iets van 30 mensen, die hebben we toen geïnformeerd en je merkt gaandeweg het jaar dat er wel steeds meer bij mij gemeld wordt dat er wel steeds meer vragen vanuit de organisatie komen van goh we hebben sus maar waarom is het zo en kunnen we dat niet anders inregelen en we krijgen mail van een ziekenhuis binnen, weliswaar via zorgmail een beveiligde omgeving, maar wel van een röntgenafdeling, de bespreking van foto's. Nou die zijn gewoon helemaal verkeerd gestuurd, weet je hoe gaan we hier mee om. Dus dat merk ik wel dat was in het begin was er echt radiostilte. Je merkt wel dat er gaandeweg meer over gecommuniceerd wordt dat er wel steeds meer mailtjes bij mij komen.

RS: Ja, dat er steeds meer mensen met vragen zitten eigenlijk.

Zorginstelling C: Ja, dat hebben we gaandeweg het jaar wel steeds meer bemerkt.

RS: Nemen jullie die vragen dan mee?

Zorginstelling C: Ja, als iets vaker voorkomt dan nemen we ze mee. Ja, want we doen ook, issues waarvan ik denk dat we daar wat mee moeten in de organisatie, die koppel ik terug in de stuurgroep en daar geef ik een advies over en dan gaat de stuurgroep de bestuurder die bepaalt dan of hij het advies wel of niet overneemt, dus dat komt wel iedere keer terug in de cyclus.

RS: Want het staat nu nog redelijk dichtbij de Raad van Bestuur, dus zij krijgen ook wel die terugkoppelingen steeds mee of niet?

Zorginstelling C: Ja we hadden bijvoorbeeld nu afgelopen weekend een datalekincident bij een bewerker. Dat neem ik ook wel gelijk op. Dan koppel ik dat terug naar de bestuurder met mijn advies daarbij van we gaan het wel of niet melden bij de autoriteit, dus die zijn heel dicht betrokken.

RS: Dus als er een datalek voorkomt zoals dit bijvoorbeeld is dan uiteindelijk de Raad van Bestuur degene die bepaald of iets gemeld wordt of ben jij degene?

Zorginstelling C: Ja, ik bepaal, ik adviseer, maar wel met dwang zeg maar om het te melden.

RS: Ja, dus dan, uiteindelijk zijn zij natuurlijk eindverantwoordelijk.

Zorginstelling C: Ja, zij zijn eindverantwoordelijk dus ik wil wel graag dat horen en dat op schrift hebben dat hij akkoord is met de melding, maar uiteindelijk adviseer ik wel dringend om dat te melden of om het niet te melden.

RS: Ja, want hoe zit het bij de Raad van Bestuur hoe hebben zij dit thema in beeld?

Zorginstelling C: Ja, alleen middels de stuurgroep.

RS: oké en daar zit de Raad van Bestuur helemaal volledig bij?

Zorginstelling C: Bij ja, we hebben nu voorlopig even een tweehoofdig Raad van Bestuur en de voorzitter zit bij de stuurgroep.

RS: Oké dus die is op die manier wordt die meegenomen in dit thema. Want hebben zij denk je ook de risico's goed in beeld?

Zorginstelling C: Ja, want daar zijn ze ook bij betrokken geweest vorig jaar was er een werkgroep die heeft de risico-inventarisatie gedaan, daar was ik toen nog niet bij betrokken. Ik heb het wel overgenomen en heb de risico's uitgezet bij de probleemeigenaren, overleg mee gehad, gevraagd hè ik heb een opdracht geschreven. Zij moesten aan de hand van die opdracht een plan van aanpak schrijven en ook die wordt iedere keer teruggekoppeld in de stuurgroep en vanuit de stuurgroep gaan ze dan weer mee in het MT.

RS: En wat kwam er dan uit die risico-inventarisatie?

Zorginstelling C: Ja, we hebben een inventarisatie gemaakt papier, techniek en gedrag ik kan het heel even uit de printer halen. Techniek, applicaties, papier en gedrag. Techniek applicaties ging dan voornamelijk over onze grootste applicatie Ons, daar staan medewerkersgegevens, maar ook de cliëntengegevens en ECD zorgplannen en dergelijke, maar daar wordt dan inderdaad gekeken van hoe kan een bewerker bij de gegevens? Zijn ze afgeschermd voor andere gebruikers? Hoe zit het met de uitval van een systeem als een netwerk uitvalt? Maar ook na wateroverlast bijvoorbeeld. Nou daar waren allemaal geen procedures voor. Dus de opdracht was van ga aan de hand van deze risico's maar ook de relaties, afhankelijkheidsrelaties, beschikbaarheidsrelatie, vertrouwelijkheidsrisico, maak daar een plan van aanpak van.

RS: Ja, precies.

Zorginstelling C: Nou en dat is dan gedaan en sommige dingen die behoeven goedkeuring van een bestuurder omdat dat dan begrotingstechnisch ook consequenties heeft. Nou ja sommige dingen kunnen niet uitgevoerd worden en dan wordt beschreven waarom we nu die keuze maken om dat nu achterwege te laten.

RS: Ja, precies. Want bij wateroverlast kan ik me voorstellen dat er iets van crisiscommunicatie bij komt kijken?

Zorginstelling C: Ja, en dan blijkt ook dat wij dat niet hebben.

RS: Ah, oké.

Zorginstelling C: Dat wij ook geen algemeen calamiteitenplan hebben. Dus naarmate je hiermee verder gaat kom je er ook achter van 'oh dat missen we ook'.

RS: Ja, dat moet misschien eerst dan zeker.

Zorginstelling C: Ja, dat moet ook dus het is wel leuk dat dat daar uit komt want we hebben dan wel een calamiteitendienst voor het weekend, maar ja als er een echte calamiteit is wat moet er dan gebeuren en hoe gaan we evacueren of wat dan ook, dat hebben we dus allemaal niet.

RS: Nee, oké want je hebt natuurlijk ook als je een melding wil doen bij de Autoriteit Persoonsgegevens van een datalek, heb je 72 uur de tijd. Ja er zijn natuurlijk ook weekenden. Dat is waarschijnlijk nu nog leeg.

Zorginstelling C: Ja, ja. Ik kijk, ik hou dat in de gaten.

RS: Ook in de weekenden?

Zorginstelling C: Nou weet ik wel dat ik was toevallig bij een Ronde Tafel gesprek van de Autoriteit dat ze die 72 uur niet zo

RS: Oh, daar ben ik ook geweest volgens mij, tenminste in Gouda.

Zorginstelling C: Oh ja.

RS: Wat grappig, ik heb jou daar helemaal niet gezien. Ja daar was ik ook bij met Udo Oelen.

Zorginstelling C: Ja en toen gaven ze wel aan dat ze die 72 uur niet zo heel dat daar ook best iets langer bij mocht zitten. Ja weet je dat is lastig want ik kreeg bijvoorbeeld afgelopen weekend dat incident. Ik keek heel toevallig vrijdagavond laat op mijn mail en toen zag ik dat er vrijdagmiddag om iets voor vijven een melding binnen was gekomen van onze bewerker. Maar dat betrof wel een incident van de donderdag, maar goed ik heb de melding pas binnengekregen op de vrijdag dus ik heb me daar maar even aan vast gehouden en ik heb toen wel zaterdag contact opgenomen met de stuurgroep en geadviseerd om maandag toch een melding te doen. Dus ik heb uiteindelijk maandagochtend die melding gedaan, dus ik neem aan dat dat prima is gegaan. Het was ook niet een heel ernstig delict ofzo maar ik vond het wel goed om te melden. En dus ja die 72 uur zal zo'n beetje in het weekend, ik check het dan maar wel even of er wat is.

RS: En met medewerkers bijvoorbeeld je kan natuurlijk ook in het weekend werken en je kan ook dingen mee naar huis nemen zijn daar veiligheidsmaatregelen voor? Bijvoorbeeld als je een USB-stick kwijtraakt?

Zorginstelling C: Beleid is bij ons om niet te werken met USB-stick. Eigenlijk is dat gewoon not done. Iedereen heeft eigenlijk toegang, kan via thuis inloggen. Dat gaat op dat platform dat beveiligd is, dus een USB-stick is not done.

RS: Dus je kan altijd overal waar je bent toegang krijgen tot dat systeem en dat systeem is dan neem ik aan wel beveiligd?

Zorginstelling C: Maar ja dan is het verhaal komt vast ook wel eens ter sprake: je bent aan het werk in het systeem met cliëntgegevens en jouw buurvrouw zit bijvoorbeeld naast jou en die kan bij jou op het scherm kijken.

RS: Ja, en dat heb je ook in de trein, dat heb je altijd.

Zorginstelling C: Ja, dat zijn van die dingen. Maar nee USB-sticks mag niet. Is opgenomen ook bij ons in de ondernemingsovereenkomst. Geen gebruik maken van USB-sticks.

RS: En sinds de Meldplicht Datalekken dan is ingevoerd sinds 1 januari 2016 merk je dan ook veranderingen? Bijvoorbeeld dat mensen er meer mee bezig zijn dan eerst?

Zorginstelling C: Ja, nu in de loop van het jaar wel, komen er meer vragen. Maar ja weet je dat heeft wel tijd nodig en ik denk ook dat de een daar meer mee bezig is dan de ander. Maar we merken nu wel dat er meer vragen via de mail binnenkomen van goh hoe moeten we nu hiermee omgaan. Laatst was er bijvoorbeeld iemand van de GGD geweest, een soort van audit/inspectie. Vooraf was toestemming gevraagd, die wilde wat inzage in cliëntendossiers en die cliënten was toestemming gevraagd. Maar op het moment dat ze er waren wilden ze ook inzage in P-dossiers van medewerkers van een betreffende afdeling om te verifiëren of diploma's in orde waren en of de VOG (Verklaring Omtrent Gedrag) aanwezig was. Daar hangt wel een raamovereenkomst boven waar ook wel in beschreven staat dat dat moet kloppen. Medewerkers zouden daarvan in bezit moeten zijn. Degene die erbij zat was er redelijk door overvallen, ja daar hebben wij ook niet echt beleid over geschreven. Wat moeten wij nu medewerkers van tevoren informeren of er inzage in een dossier is ja of de nee en je kan het niet altijd informeren want soms is het steekproefsgewijs. Nu is het achteraf gedaan. Medewerkers waren daar wel een beetje verbolgen, niet iedereen, maar een aantal waren daar wel een beetje over verbolgen. Ja daar moeten we wel iets mee.

RS: Ja, want voor jullie als instelling wat zijn dan volgens jou de grootste risico's die je loopt als er een issue is een datalek bijvoorbeeld of een privacy issue?

Zorginstelling C: Nou, weet je ik ben niet zozeer bang voor een datalek, dat kan ons allemaal overkomen. Ik ben er wel van overtuigd dat als je de dingen maar transparant en helder hebt en er gewoon duidelijk in bent en ook in de communicatie naar buiten. Tuurlijk is het heel erg vervelend als het gebeurt en het is heel vervelend als een medewerker een laptop in zijn auto laat staan en zijn auto wordt opengebroken of weet je wat dan ook, maar uhm zolang wij kunnen aantonen dat wij onze omgeving goed beveiligd hebben en ook maar gewoon duidelijk zijn in het melden ook naar de betrokkene eventueel als dat noodzakelijk is, denk ik dat je op zich niet zo'n groot risico loopt. Wel als je het gaat achterhouden en gaat verzwijgen en denkt van we branden onze vingers er niet aan, we houden onze mond maar dicht.

RS: Dat zit dan inderdaad meer een beetje op het vertrouwen, de reputatie.

Zorginstelling C: Ja, daar kan je denk ik hele grote schade aan lijden als het bijvoorbeeld groot in de krant komt wat de laatste tijd best veel bij gemeentes voorkomt.

RS: En zorginstellingen ook.

Zorginstelling C: En zorginstellingen ook. Ja weet je dat wil je niet. Ja weet je je kan heel veel dingen noemen. Maar ik denk ook transparant naar elkaar, maar ook naar ketenpartners. Ja weet je als wij dat voorbeeld dat ik net noemde, als wij van een ziekenhuis gegevens doorkrijgen die gewoon niet voor ons bestemd zijn en waar gevoelige informatie in staat. Weet je, je kan het heel hoog op gaan spelen, maar je kan ook mekaar gewoon helpen en zeggen hee jongens, wees even alert hè. Of als er een overeenkomst opgestuurd wordt en er zit achter een andere overeenkomst voor een hele andere cliënt van een hele andere zorginstelling. Ik denk dat je eerst moet zoeken naar gewoon ook een samenwerking.

RS: Ja.

Zorginstelling C: Niemand zit te wachten op een boete van acht ton.

RS: Nee, dat je gewoon kan terugkoppelen naar elkaar van goh dit is mij opgevallen.

Zorginstelling C: Ja, kijk het moet niet 100 keer per week voorkomen natuurlijk, want dan heb je zelf ook wel een keer een probleem, dan wordt het ook jouw probleem dat moet je denk ik niet willen. Ik denk dat dat het grootste risico voor onze organisatie is, hoe medewerkers ermee omgaan.

RS: Ja.

Zorginstelling C: Weet je er wordt nog heel veel via Whatsapp verstuurd want dat is makkelijk en dat is ook een risico waar wij ook naar moeten kijken dat niet al onze medewerkers dus een eigen account hebben, want hoe moeten medewerkers dan communiceren? Dan gaat het via de Gmail, ja dat is dus. Daar moet je dus keuzes in gaan maken.

RS: Ja, en dat kost natuurlijk ook weer geld.

Zorginstelling C: Ja, wat er dan niet is, want dat blijft een lastig probleem.

RS: Ja, het zou eigenlijk handig zijn als ze daar een soort algemene applicatie voor hebben. Ik heb daar wel iets over gelezen laatst trouwens dat ze de Ipads zo hadden geïnstalleerd dat je alleen toegang kon krijgen tot bepaalde applicaties. Dus Gmail en dergelijke daar kan je dan gewoon niet op.

Zorginstelling C: Nee, maar dan doen ze het wel via een omweg thuis via Gmail en dergelijke.

RS: En zou je dan zeggen dat privacy op dit moment in jullie organisatie een hoge prioriteit heeft of een lage?

Zorginstelling C: Ik denk, nee denk is niet het goede woord, ik vind dat het een hoge prioriteit heeft bij heel veel mensen, maar ik denk bij de medewerkers die echt zorg willen verlenen dat dat niet zo heel erg meespeelt.

RS: Ja.

Zorginstelling C: Dat die toch wat, ja of er niet bij stil staan of weet je vroeger deden we het ook zo dus waarom zouden we het nu niet zo doen, de verandering is dan heel lastig. Aan de andere kant denk ik ook dat je ook niet te gespannen ermee om moet gaan.

RS: Want hoe is er bijvoorbeeld iets naar medewerkers gecommuniceerd over die Meldplicht Datalekken?

Zorginstelling C: Nieuwsbrief.

RS: Want als hen iets opvalt of iets dergelijks kunnen zij dat dan intern melden?

Zorginstelling C: Ja, er is een interne meldingsprocedure voor. Ja, staat ook op intranet, daar hebben we een intern meldingsformulier. Dat wordt nog niet zo vaak gebruikt. Het merendeel gaat toch via de mail gegevensbescherming. Daar komt het dan op binnen of op mijn persoonlijke mail. Maar er is wel een intern formulier voor.

RS: Oké dus dat is er dan inderdaad wel. Want in hoeverre denk je dan dat communicatie zou kunnen bijdragen aan het inperken van risico's binnen de organisatie?

Zorginstelling C: Uhm, ja ik denk dat zij daar wel een rol in kunnen hebben. Alleen dat is bij ons toch wel weer wat anders belegd. Communicatie is hier wat meer ondersteunend aan en de rest moet je eigenlijk zelf maar doen. Het is niet echt zo dat zij, ja weet je je kan ze oproepen als je ze nodig hebt ergens mee, maar zij nemen niet het voortouw van we gaan een campagne opstarten ofzo met dat als onderwerp. En dat is ook weer een beetje omdat dan die prioriteiten weer anders liggen.

RS: Ja, want waar liggen die prioriteiten dan bijvoorbeeld wel?

Zorginstelling C: Ja, dat is voornamelijk ook wel bij uitvoerende, folders up to date houden, foto's.

RS: Ja, precies, dus eigenlijk meer extern gericht dan intern.

Zorginstelling C: Ja, nu wel. En ik weet daar zijn ze dan mee bezig, onze afdeling communicatie is bij ons altijd een afdeling geweest die dan daaronder hing en dan daaronder die had nooit echt een vaste plek. Dus veel wisseling ook in leidinggevenden en afdelingen. Ja er zit nu nog maar één persoon en dan een externe, maar ja die heeft andere taken. Dus dat is ja een beetje een ondergeschoven kindje nu.

RS: Ja, dus er is eigenlijk geen echt duidelijke plek voor communicatie. Ja, dat maakt het natuurlijk ook ontzettend lastig, want ja dan wordt het natuurlijk ook moeilijk om vanuit communicatie, of als communicatieafdeling of medewerker zelf met initiatieven te komen.

Zorginstelling C: Nou nee, daar is geen ruimte voor. Ik vind dat wel jammer hoor, ik denk namelijk best dat ze een grote rol kunnen bijdragen. Ja nu moet je zelf een beetje het wiel uit proberen te vinden en dan ja, is het dan goed, ja ik weet niet of het goed is, maar ja je probeer het beste te doen en je haakt een beetje aan bij andere organisaties en je informeert eens van 'goh hoe zijn jullie bezig' zeg maar.

RS: Zijn er ook samenwerkingen bijvoorbeeld of regionale overleggen?

Zorginstelling C: Nee, niet dat ik weet. Ik heb laatst wel een gesprek gehad met de gemeente en die had ook zoiets van ja eigenlijk moeten we toch een soort ketenoverleg ofzo initiëren. Dus ik zei van nou volgens mij is dat heel goed om het initiatief bij de gemeente te leggen, want die is natuurlijk ook verantwoordelijke voor heel veel zorginstellingen of ja ketenpartners, maar goed diegene zat ook met het ene been in de ene functie en met het andere been in de andere functie maar die wilde dat wel meenemen want die miste dat ook. Nou ja ik ben dan wel een keer bij een ronde tafel geweest dat was georganiseerd door heliview en daar zaten wel, ja dat was meer richting Enschede was dat toen, maar dat was wel interessant gewoon even met elkaar praten van hoe ga je ermee om en ik merk dat dat communicatie intern gewoon echt een heel moeilijk ding is hoor.

RS: Ja, heb ik ook gemerkt op de congressen waar ik geweest ben inderdaad. Voor ik deze interviews ging afnemen, wilde ik natuurlijk eerst wel weten waar mensen mee zitten, want anders kun je natuurlijk ook geen gerichte vragen stellen als je niet genoeg over het thema weet. Het is natuurlijk een lastig punt, want ja in principe: medewerkers zijn wel de groep die je moet hebben, want het is wel waar de meeste risico's vandaan komen eigenlijk. Hebben jullie ook een extern meldpunt? Dat mensen van buiten de organisatie als hen iets opvalt kan natuurlijk ook voorkomen dat patiënten een melding willen doen omdat zij een mail binnen krijgen die niet voor hen bestemd is.

Zorginstelling C: Ja, nee dat hebben we niet voor extern, ja dat staat op onze website misschien, maar dan moet ik even het antwoord schuldig blijven. Het zou kunnen dat we in ons privacyreglement dat het wel benoemd staat en het mailadres gegevensbescherming. En we hebben wel bij de invoering van het ECD, daar waren natuurlijk ook wel veel vragen over van cliënten met name van oudere cliënten hoe zit dat dan en mijn gegevens staan in de cloud en hoe moet ik dat dan zien? Daar hebben we wel een informatiefolder van gemaakt hoe wij daarmee omgaan en daar staat het mailadres ook wel genoemd.

RS: Dus ze weten er wel van.

Zorginstelling C: En ze weten ook wel dat ze hun eerste verantwoordelijke kunnen aanspreken.

RS: En is er bijvoorbeeld extra communicatie-inzet geweest intern dan wel extern na aanleiding van de meldplicht?

Zorginstelling C: Nee, behalve de nieuwsbrief over de meldplicht datalekken en een stuk op intranet, waar dan het plan van aanpak beschreven staat. En ja ik heb op intranet een stukje geschreven dat die wet is ingegaan en nou ja een informatiebijeenkomst. Dat was dan eind januari, we hebben ook net de medewerkersbijeenkomst achter de rug dat doen we 2x 2 jaarlijks en dan heb je vijf gebieden waar we zitten organiseren we medewerkersbijeenkomsten en dan is dit onderwerp uhm werd ook aangetipt.

RS: Oké en dat is dan één keer in de zoveel?

Zorginstelling C: Ja, één keer per half jaar. Meestal is dat net na de zomer en dan begin van het nieuwe jaar.

RS: En dat is dan een bijeenkomst voor alle medewerkers in de organisatie?

Zorginstelling C: Ja, iedereen wordt uitgenodigd. Hele wisselende opkomst, je moet niet denken dat er honderden mensen zijn, maar goed. Die bijeenkomst zijn we gestart omdat de werkoverleggen eigenlijk wat geskipt werden vanwege reistijd en productiviteit. En nou ja daar worden actuele zaken besproken, maar dat gaat ook over de financieringssituatie van de organisatie, een beetje dat soort onderwerpen.

RS: Ja een soort oudejaars iets, jaarrekeningen en dergelijke.

Zorginstelling C: Ja, ja.

RS: Oké want je hebt dan al die verschillende afdelingen, zitten die wel ergens in dit gebouw die hoofden daarvan?

Zorginstelling C: Ja, dat zit allemaal wel hier.

RS: Want die medewerkers bijvoorbeeld zoals wijkverpleegkundigen en dergelijke hebben die een plek of zijn die gewoon altijd dynamisch over de regio?

Zorginstelling C: Ja voornamelijk. Wij hadden voorheen altijd rayonkantoren, maar daar hebben we een heel aantal van afgesloten, dus de plekken worden steeds minder. Maar er zijn nog wel een aantal kantoren waar zij nog wel terecht kunnen, maar het meeste is dynamisch. Want als ze naar kantoor gaan mogen ze daar eigenlijk geen tijd voor schrijven, dus eigen tijd, dus het merendeel gaat inderdaad dynamisch.

RS: Oké dus in principe: ze kunnen online hun diensten zien?

Zorginstelling C: Ja, dat gaat via dat Ons.

RS: En daar staat in wanneer ze waar moeten zijn?

Zorginstelling C: Ja, hun rooster.

RS: En die mensen worden dan ook gewoon gebeld door de patiënten als er iets is?

Zorginstelling C: Ik weet niet of zij rechtstreeks benaderd kunnen worden, ze zullen het nummer in hun telefoon hebben en anders gaat het bij ons via de zorgcentrale, die is ook dag en nacht bereikbaar.

RS: Oké dus dat zit op die manier. Dus die mensen zijn dan ook lastiger te bereiken natuurlijk, omdat ze niet op één plek zitten.

Zorginstelling C: Nee, nee. Nou die wijkverpleegkundigen hebben dan wel één keer in de zoveel tijd een teamoverleg met hun leidinggevende, maar ik weet niet precies hoe vaak.

RS: Want als er een melding binnenkomt wordt de betreffende medewerker die die melding gedaan heeft daar dan ook verder in mee genomen?

Zorginstelling C: Ja, ja. Er volgt altijd een terugkoppeling. Hoe we ermee om zijn gegaan.

RS: Misschien ook nog wel extra vragen of iets dergelijks?

Zorginstelling C: Ja, als er extra vragen zijn bel ik dan ook vaak.

RS: Ja, dat formulier is vrij uitgebreid op de website.

Zorginstelling C: Ja dat klopt, maar er is wel veel, we hadden van de week dan die melding, dan krijg ik van de bewerker al helemaal een ingevuld formulier, die ik eigenlijk één op één kan overnemen.

RS: Ja, dus dat is met een bewerker ook anders.

Zorginstelling C: Wij hebben zelf ook nog geen datalek gehad dat we moesten melden. Maar goed van een bewerker hebben we al wel moeten melden inderdaad.

RS: En wat denk je dingen die medewerkers zouden gaan motiveren om te gaan melden? Ik kan me voorstellen dat ze een beetje terughoudend zijn daarin.

Zorginstelling C: Ja, dat is bij ons ook lastig, want dat is bij ons net zoals een MIC-melding of een MIM-melding. Dat wordt bij ons nauwelijks gedaan.

RS: Ja dat zijn van die kwaliteitsmeldingen?

Zorginstelling C: Ja MIC is Melding Incident Cliëntenzorg en MIM is Melding Incidenten Medewerker. Dat wordt bijna niet gedaan, omdat men aangeeft ja we vergeten het of we denken er niet aan of ja het is te lastig om het formulier te vinden. Ja weet je verzint 10 excuses geen idee.

RS: Hoe komen jullie erachter waarom mensen dat niet invullen?

Zorginstelling C: Nou ja want op een gegeven moment ga je kwaliteitsuitvraag doen en dan denk je op zoveel medewerkers en met zoveel cliënten en dan maar zo weinig meldingen dat kan nooit goed zijn.

RS: Nee, precies.

Zorginstelling C: En dan ga je dat terugkoppelen en ja weet je we hebben hier ook bijvoorbeeld de MIC-commissie en daar is inderdaad naar gekeken van hoe kan dit anders en dan is er weer ander beleid en het verandert niet. En kwaliteit is hier, het is altijd goed hoor, we hebben altijd een hoog cijfer voor kwaliteit en ook bij de CQ index en noem maar op. Maar het is altijd wel een dingetje en dit is ook een dingetje. We willen dit koppelen aan kwaliteit, omdat wij vinden dat kwaliteit iets moet zijn wat jij in je hebt als zorgverlener. Maar medewerkers ervaren het, vooral de uitvoerende echt als een dingetje.

RS: Ja, eigenlijk een beetje als iets vervelends.

Zorginstelling C: Droog, saai.

RS: Ja, want zij krijgen dan bijvoorbeeld als je een nieuwe medewerker hebt die krijgen dan bijvoorbeeld die procedure voor het datalekken?

Zorginstelling C: Ja, dat is nu wel de bedoeling. Dat willen we nu wel opnemen bij indiensttreding of bij de algemene gedragscode dat iedereen dat gewoon krijgt.

RS: Ja, want op dit moment hebben medewerkers wel die gedragscode?

Zorginstelling C: Ooit een keer gekregen, een keer een 'gebruik ICT' e-mail en daar zet je dan ook een keer een handtekening voor. Nou negen van de tien mensen leest het waarschijnlijk niet. Dus dat willen we ook anders. We willen die algemene gedragscode straks ook door de bestaande medewerkers allemaal opnieuw laten tekenen.

RS: En die gedragscodes en dergelijke en je hebt natuurlijk daarnaast het privacyreglement op wat voor wijze wordt dat?

Zorginstelling C: Ja, dat kunnen mensen lezen op intranet, maar dat is niet actief.

RS: Nee.

Zorginstelling C: Ja, het staat daar.

RS: Want ik kan me voorstellen je kan een beetje een vergelijking trekken met al die vreselijke meldingen die je krijgt van als je weer een app gaat downloaden of iets dergelijks, daar gaat natuurlijk niemand gaat dat lezen.

Zorginstelling C: Ja, iedereen klikt door.

RS: Ja dus hoe zou je er dan voor kunnen zorgen dat mensen wel zoiets gaan lezen of er iets mee gaan doen?

Zorginstelling C: Ja, we willen het ook onderdeel gaan laten uitmaken van het functioneringsgesprek. Gewoon een agendapunt: het hoort erbij net zoals dat je een opleiding bespreekt tijdens je functioneringsgesprek. We willen het niet als wijzende vinger, maar gewoon van hoe ga je nou om met. Je krijgt het nooit waterdicht, want je kan mensen laten tekenen of je kan mensen een vinkje laten zetten, maar je kan nooit toetsen of je het nou daadwerkelijk hebt gelezen dat is heel moeilijk om een vinger op te krijgen. Ja, net zoals weet je melden mensen alles wel? Ja ze melden niet alles, dat weet ik zeker.

RS: Ja, dat zullen ze niet doen inderdaad, maar ja je kan natuurlijk wel bevorderen dat ze het gaan doen of erachter proberen te komen hoe gaan jullie met die gegevens om.

Zorginstelling C: Ja, we hebben nu dan in november die workshop staan en dat hebben we ook uitgezet hoor van we willen niet droge stof aandragen we willen eigenlijk gewoon aan de hand van stellingen en aan de hand van praktijkcasussen een interactieve sessie hebben. Dus we hebben de vraag ook uitgezet van waar loop jij in de praktijk nu tegen aan. Nou en daar zie je wel dat daar wel reacties op binnen komen, want dat alleen maar stof aandragen en wetten en toestanden ja weet je daar zit niemand op te wachten.

RS: En wat voor soort training is dat dan aan wie wordt die gegeven?

Zorginstelling C: Dat is wel weer wat aan de top. Dus het MT, de leidinggevenden, de afdeling finance en control, de ICT-afdeling vanuit daaruit, maar dat kan je aan de hand van stellingen natuurlijk wel leuk doen, kunnen zij het weer meenemen in hun werkoverleg en dan wellicht dezelfde stellingen gebruiken of diezelfde praktijkcasussen.

RS: Ja, je moet ook natuurlijk ergens beginnen. En je was dan ook bijvoorbeeld bij die NVFG bijeenkomst geweest en daar was dan Udo Oelen van de Autoriteit Persoonsgegevens. Maar hoe kijk jij eigenlijk tegen die rol aan van de Autoriteit Persoonsgegevens?

Zorginstelling C: Uh, ja hoe kijk ik tegen die rol aan. Ik vind ze nog niet heel sterk. Ik vond ook dat tijdens die bijeenkomst ze zelf ook niet heel sterk naar voren kwamen, omdat er nog teveel ook onduidelijkheid was, wat je dan merkt is dat je de ene dag belt en je krijgt Jan aan de telefoon en de volgende dag krijg je Pietje, dat ze dan beiden een ander antwoord geven. Ikzelf vind dat hun bereikbaarheid heel slecht is. Ik heb ze een paar keer gebeld en dan kreeg ik een bandje dat er een probleem was of ik weet niet hoe lang ik in de wacht heb gestaan, ze zijn niet per mail bereikbaar. Dat vind ik ook heel vervelend, alleen maar de ochtenduren. Ja, ik kijk er niet tegenop ofzo. Ik vind autoriteit een fantastische naam, maar ik heb niet zoiets van poehpoeh ik lig er wakker van.

RS: Maar dus niet makkelijk benaderbaar in ieder geval?

Zorginstelling C: Nee, absoluut niet.

RS: Ja, vreemd met dat mailadres.

Zorginstelling C: Er zijn ook heel veel goede dingen hoor, zoals ik vind hun website goed want als je zoekt op bepaalde onderwerpen krijg je best snel je informatie, kan je boven water halen. En ik moet zeggen dat ik vind dat zij zelf wel wat autoriteit uitstralen in die zin van je durft bijna geen vraag te stellen telefonisch omdat je denkt van oeps weet je wel als ik nu die vraag stel waar ik zelf dan niet uitkom dan krijg je meteen een vinkje bij je naam en dan gaan ze daar naar kijken. Dus ik vind transparantie, dat zou denk ik beter kunnen of anders kunnen.

RS: Ja, ik merkte dat ook bij die bijeenkomst dat niemand eigenlijk zei waar die vandaan kwam.

Zorginstelling C: Ja, iedereen was een beetje zo van

RS: Ik vond dat heel erg bijzonder, we zitten hier toch om antwoorden te krijgen, juist hebben we praktijkvoorbeelden nodig waar je wel specifiek kunt benoemen waar het omgaat zodat we wel hier stappen in kunnen zetten.

Zorginstelling C: Ja, iedereen is dan toch een beetje en dat snap ik he want ik heb ook begrepen dat zij dit ook niet zo heel snel doen. Dat ze dit ook nog nooit eerder hadden gedaan zo'n bijeenkomst waar zij bij aanwezig waren. Terwijl ik juist denk, ja je moet het zo zien. We moeten niet denken met z'n allen dat is de grote politieagent daarboven waar we allemaal bang voor moeten zijn. Ik bedoel zij moeten de wetten handhaven, de regels, wij moeten ons daar als organisatie aan proberen te houden, maar laten we vooral heel open en duidelijk tegen elkaar zijn want ja, niemand zit te wachten op, zij zitten ook niet te wachten op een boete uitdelen, want als zij een boete uitdelen daar krijgen zij ook gedoe mee of gedoe mee, dan gaat iedereen ook zeggen ja nou ze hebben hun natje gehaald.

RS: Ja, ze hebben natuurlijk een bewuste keuze gemaakt meer als soort toezichthouder op te treden en niet als advies/raadgevend orgaan. Daar valt over te twisten of dat een goede keuze is geweest en de boetes zijn natuurlijk nog niet aan de orde geweest.

Zorginstelling C: Nee, ongetwijfeld zal er snel eentje gaan komen.

RS: Is ook misschien niet heel handig om meteen te doen, want hoe meer boetes er worden uitgedeeld, hoe minder mensen gaan melden.

Zorginstelling C: Ja dat is de andere kant van het verhaal, die boetes zijn zo enorm hoog. Ja weet je als je als organisatie een boete krijgt dan is het einde. Tenminste bij zorginstellingen gaat het nu niet zo heel fantastisch allemaal.

RS: Nee, dat zijn geen leuke boetes.

Zorginstelling c: Nee, dat is niet leuk.

RS: En je hebt nu natuurlijk de Wet Meldplicht Datalekken en de Autoriteit Persoonsgegevens. We bevinden ons eigenlijk in een soort tussenfase in de richting van de Europese Verordening in 2018 officieel gehandhaafd mag worden. Je krijgt dan 2 jaar de tijd als organisatie om eraan te gaan voldoen. Hoe denken jullie dat jullie daarin staan tegen die tijd?

Zorginstelling C: Nou wij hadden een mooi schema, had ik gevonden en daar stond dan in wat zijn nu de grootste veranderingen, maar naar aanleiding van de Ronde Tafel bijeenkomst heb ik hier het advies gegeven om vooral nu nog even niets te doen, want de autoriteit gaf zelf aan dat het voor hen ook nog niet helemaal duidelijk is wat nu de kaders zijn en wat voor richtlijnen zij daaraan gaan hangen en dat zij ook met iets naar buiten willen gaan komen. Dus ik heb hier als advies gegeven ja weet je we kunnen het beste jongetje van de

klas willen zijn en ons helemaal daar nu op gaan richten, maar zolang de autoriteit daar nog niet echt verder mee naar buiten is getreden, laten we het even zo houden. Want door allerlei commerciële partijen wordt je benaderd wordt je doodgegooid bijna met trainingen en cursussen en opleidingen, maar dan denk ik laten we eerst eens duidelijk hebben wat zo'n autoriteit daar nou mee wil beogen.

RS: Ja, want de Autoriteit Persoonsgegevens die heeft dus nog niet op hun website hierover staan?

Zorginstelling C: Vond ik bijzonder om te horen tijdens die bijeenkomst. Ja, weet je zolang zij daar nou nog niks over hebben.

RS: Ja, want die regels die zijn er natuurlijk wel gewoon en daar zijn ook heel veel dingen aan te koppelen. Dingen die je op orde moet hebben tegen die tijd.

Zorginstelling C: Ja, maar volgens mij speelt er nog wel is er nog wel wat variatie in in te brengen. Natuurlijk zijn wij, we hebben natuurlijk mij aangesteld als FG, alle gegevensverwerking moet gedocumenteerd worden wat natuurlijk eerst niet zo was. Daar zullen we een slag in moeten maken want dat is nu nog niet. Als ik daar kijk naar het formulier dat de autoriteit handhaaft dan denk ik van nou dat is zo'n stapel papier, waar ze dan wel een programmatje voor hebben, maar ik weet zeker als ik dat hier ga uitzetten dat de helft van de mensen niet weet wat ze moeten invullen dus daar moeten we eerst eens kijken of we daar een schift in kunnen maken en dan misschien geven zij daar zelf ook wel een ander handvat aan. Dus ja, weet je, we hebben zoiets nu van, we wachten heel even af wat de autoriteit hiermee gaat doen.

RS: Nee, logisch dan ook inderdaad. Ik denk dat ik alle thema's heb behandeld, even kijken of ik niet nog iets heel belangrijks ben vergeten. Nee, volgens mij niet. Bedankt voor je tijd.

5.4 Uitwerking interview zorginstelling D

RS: Haalt voorbeeld aan van privacytest die offline gehaald werd wegens privacyschending. Maar goed het is natuurlijk een heel actueel thema in Nederland. De functie van privacy officer is natuurlijk vrij nieuw. Hoe ben je bijvoorbeeld bij deze functie terechtgekomen?

Zorginstelling D: Ja, eigenlijk omdat ik als jurist hier werk en eigenlijk als je kijkt naar het functieprofiel van FG dan zit daar best heel veel overlap in en als je dan verder in de zorginstelling kijkt van ja waar kun je het beleggen dan leek dit de meest aangewezen plek.

RS: Ja.

Zorginstelling D: Het onderwerp privacy en beroepsgeheim en dat soort zaken, ja dat lag toch al bij mij, dus het is in die zin een heel erg pragmatische keuze geweest om het aan de functie van de jurist te koppelen.

RS: Oké en hoe zit dit in de rest van de organisatie verworven? Valt dit onder een afdeling of?

Zorginstelling D: Ja, dat is een spannende vraag, want we hebben net een reorganisatie gehad en uhm ja het meest duidelijk is; ik val vrij direct onder de Raad van Bestuur. Er zit nog een directiesecretaris zit daar dan nog functioneel tussen zeg maar voor de arbeidsvoorwaardelijke zaken enzo, maar ik zit niet meer bij een organisatieonderdeel, maar het zit heel dicht tegen de Raad van Bestuur.

RS: Oké het is natuurlijk ook een onafhankelijk functie.

Zorginstelling D: Ja en dat is ook de reden waarom ook nu na de hele reorganisatie ervoor gekozen is om de functie jurist ook daar te laten, omdat je dan toch het meest onafhankelijk kunt functioneren in de organisatie.

RS: Ja, want als er dan bijvoorbeeld beleid opgesteld wordt omtrent dit thema, ik weet niet of dat al de zaak is hier, maar gaat dat dan vanaf jou, neem jij daar het initiatief voor of gaat dat ergens anders in de organisatie bijvoorbeeld bij de Raad van Bestuur?

Zorginstelling D: Ja, kijk privacy is natuurlijk in de GGZ altijd al een belangrijk thema geweest, dus het is niet zo dat er nu in één keer nu de nieuwe wetgeving er is, dat iedereen zo zit van 'oh we moeten van alles', uhm, ja ik ben zelf als het om nieuwe wetgeving gaat dan vaak wel degene die daarop wijst of initiatief neemt of stukken daarover schrijft, uhm ja verder kan het van allerlei kanten komen waar privacy speelt. Ik denk wel dat nu met de Wet Datalekken, maar ook de hele ontwikkelingen rond bestuurlijke verantwoordelijkheid, dat dit thema wel een soort professionaliseringsslag meemaakt. Zeg maar dingen die ik vind dat ze vrij hapsnap een beetje adhoc geregeld zijn in een organisatie daar gaat nu meer gekeken worden naar het integrale beleid zeg maar. Dus we hebben wel allerlei documenten over privacy, beroepsgeheim, over wat je wel en niet mag en moet, maar ja het is natuurlijk zo breed, het zit natuurlijk overal in dat je ook het totaalplaatje wil.

RS: Ja, want je hebt natuurlijk privacy en je hebt de bescherming van persoonsgegevens. Maken jullie daar nog onderscheid in?

Zorginstelling D: Nou, ja, ik zou bijna zeggen het liefst zo min mogelijk. Kijk privacy is natuurlijk een enorm containerbegrip, maar aan de andere kant als je dan voor mensen onderscheid gaat maken tussen persoonsgegevens en privacy dan wordt het voor de medewerkers weer heel lastig.

RS: Ja.

Zorginstelling D: Dat merk ik nu al met datalek, daar zitten we nu ook, daar zijn we bezig met een voorlichtingscampagne daarover om mensen er ook van bewust te maken dat ze dingen moeten melden en ja dan moet je gaan uitleggen ja wat is een persoonsgegeven en dan weten mensen het wel maar als je dan een definitie opschrijft, daar worden mensen niet gelukkig van.

RS: Nee, want wat voor soort medewerkers werken hier allemaal?

Zorginstelling D: We zijn met ongeveer 2400 medewerkers nou weet ik het niet precies maar volgens mij zijn iets van tussen de 1400 en 1600 daarvan hulpverleners, ja dat varieert van psychiater, psycholoog, verpleegkundigen, agogen, verzorgenden en verder ja secretarieel staf.

RS: Maken jullie nog onderscheid in die groepen hoe je ze benadert? Ze krijgen natuurlijk die privacyregels.

Zorginstelling D: Ja, kijk, ja hoe moet ik dat zeggen. We hebben een elektronisch documentensysteem en daar staat alle informatie daar staan alle beleidsafspraken en regels in. Nu is dat natuurlijk een vrij statisch iets, daar moeten mensen al de moeite voor nemen om in te gaan kijken en die richten zich, de meeste regels richten zich toch wel op de zorgverlening en er is een handboek administratie en daar staan ook wel dingen in voor administratieve staf enzo.

RS: Oké en je had het bijvoorbeeld over een voorlichtingscampagne wordt die vanuit jou geregeld of?

Zorginstelling D: Nou ja het is goed om even uit te leggen die FG functie is ongeveer een jaar geleden ingesteld, ja toen heb ik ook aangegeven dat is ook belangrijk dat we weten waar we nu staan hè want ja ik kan wel zogenaamd toezicht gaan houden, maar als we niet eens weten wat de nulmeting is, want ik wist natuurlijk vanuit mijn functie als jurist wel heel veel aspecten, maar het totaalplaatje was er niet. Dus we hebben een extern bureau een privacy impact assessment laten doen. Nou daar hebben ze een eerste stap in gedaan, een soort grof overzicht en één van de zaken die daaruit kwam was inderdaad dat er een soort awarenesscampagne moest komen. Dus daar zijn we nu met de afdeling communicatie net in gestart om dat op poten te zetten, dus dat heeft nog niet een echte inhoud, maar toevallig zit dat externe bureau dat daar onderzoek gedaan heeft, zit vandaag ook hier weer voor stap twee en dan even nog meer specifiek kijken naar voldoen we aan de wettelijke eisen en normen vanuit de NEN enzo en de Wet Datalekken en nou ja noem maar op. Dus dan is er ook een soort totaalplaatje straks van waar schieten we nog tekort en ik denk dat we in technische zin zaken wel redelijk goed voor elkaar hebben hè. Je kunt hier echt niet zomaar een patiëntendossier in hoor daar moet je echt wel voor geautoriseerd zijn en zoveel wachtwoorden ingevuld hebben, maar de awareness, dus het informeren van mensen van wat mag je nou wel en wat mag je nou niet, het toezicht en het sanctiebeleid, die punten daar vind ik zelf van daar moeten we nog wel mee aan de slag.

RS: En heeft de Raad van Bestuur dat ook een beetje in beeld zo op diezelfde manier?

Zorginstelling D: Uh Ja, want we hebben een afdeling informatiemanagement, met dat hoofd zet ik het nu op en we hebben inmiddels maandelijks overleg met één van de directeuren met één van de bestuurders over nou ja wat is nu de stand van zaken en daar zit natuurlijk het mechanisme achter, daarachter zit de Raad van Toezicht die ook willen weten wat is de stand van zaken. En dat is wel dat merk je bij zo'n Wet Datalekken er wordt met hoge boetes gedreigd en dan ontstaat er een soort schrikeffect ook bij bestuurders zo van hebben we het wel op orde.

RS: Ja, dus dat is één van de risico's natuurlijk die je hebt de boete. Zijn er nog andere risico's voor jullie als instelling?

Zorginstelling D: Ik denk het grootste risico als instelling is natuurlijk de imagoschade die je op kunt lopen en eventueel de financiële schade maar goed dat zou dan zijn als iemand een schadeclaim in gaat dienen, maar het zou natuurlijk plat gezegd heel gênant zijn als patiëntgegevens op straat komen te liggen.

RS: Zie je wel veel gebeuren natuurlijk, misschien ook niet altijd te voorkomen.

Zorginstelling D: Uhm, nee, nou de grootste kwetsbaarheid hè als wij daar met de interne deskundige over nadenken is de menselijke factor. Technisch is het wel dichtgespijkerd, zelfs als je er het beleidsdocument op na slaat dan denk je nou dat ziet er allemaal wel netjes uit, maar mensen moeten zich er ook naar gedragen, dus dat betekent dat mensen moeten weten wat ze wel en niet mogen en dan ook nog doen. Een simpel iets, nou er staat duidelijk opgeschreven dat je geen persoonsgegevens naar privé-emailadressen moet sturen, alles moet binnen het netwerk van ons blijven. En ik hoorde nu gisteren toevallig weer dat vanuit hoger management nog daar onbekendheid mee was dat er tegen een medewerker werd gezet, nou dan stuur je het toch even naar je huismailadres. Technisch lukte het intern even niet dan was het van nou dan stuur je het toch even.

RS: Ja, ja precies.

Zorginstelling D: Nou dan val ik bijna van mijn stoel: hoe kan het dat iemand vanuit hoger management dit zegt? Dit is voor mij zo'n basisregel, waarvan ik best wel eens begrijp dat er misschien ook wel bewust een keer voor gekozen wordt om dat niet te doen, maar nou ja dan denk je nog dan overtreden mensen bewust de regel, maar onbewust regels overtreden, ja dan wordt het wel, dan moeten we toch wel aan de slag om het mensen helder te maken.

RS: Ja en dat doen jullie bijvoorbeeld met die voorlichtingscampagne en is die specifiek gericht op de datalekken of meer op het algemene privacy?

Zorginstelling D: Dat zal beiden zijn, ja we hebben nu één gesprek gehad met communicatie en nou ja het woord campagne wordt al meteen is dat nou wel de juiste term, want campagne is kortdurend begrijp ik in jullie termen in jullie vakgebied.

RS: Nou ja, maar het is natuurlijk al voorlichting is iets wat je op verschillende manieren kan invullen natuurlijk.

Zorginstelling D: Nee precies, dus het zal een campagne worden met verschillende aspecten, waarin we het principe van datalekken en het melden ervan op een redelijk eenvoudige manier nu naar voren willen brengen door toch heel kort uit te leggen van nou ja wat is het en wat doe je? Bij wie meld je dat? En wat gebeurt er dan mee? Maar het hele privacyaspect dat zal een doorlopende informatie moeten zijn.

RS: Want is er nu, wordt er nu al iets aan medewerkers overgedragen bijvoorbeeld over privacy?

Zorginstelling D: Nou, niet heel veel anders dan wat ik zei via dat digitale documentatiesysteem en ikzelf word wel eens uitgenodigd op een afdeling om iets erover te vertellen en dat gaat dan meestal vanuit de regels vanuit het beroepsgeheim zeg maar, wat mogen we nou wel delen en wat niet.

RS: Ja, oké dus dan zijn ze daar zelf misschien onzeker over en dan willen ze graag…

Zorginstelling D: Nou ja weet je over communicatie gesproken wat dat betreft gemeentes die willen graag dat wij heel veel delen met andere partijen en zij hebben ook een partij die zij inhuren en die hebben een hele mooie leertuin en die promoten eigenlijk dat je veel meer kunt delen dan wat wij als gezondheidszorgveld vinden. En dat is dus ontzettend moeilijk want de mensen op de werkvloer worden er nu mee geconfronteerd met vanuit de ene kant mensen vanuit de gemeente die zeggen van 'goh jullie mogen veel meer delen hoor het is ons verteld door een jurist en het mag allemaal', terwijl ja, ze ook van mij horen, maar ook van de brancheverenigingen en de beroepsvereniging van nee dat is niet zo je hebt je gewoon te houden aan de regels van het beroepsgeheim en dan zie je mensen dus verschrikkelijk worstelen want ja je zit wel aan tafel met elkaar en de één zegt 'goh vertel mij eens even ken jij die persoon?' En dat is al de basisvraag waarvan degene met beroepsgeheim al moet zeggen 'ja joh dat mag ik je niet zomaar vertellen of ik iemand ken of niet'. Het feit alleen al dat iemand bij onze instelling ingeschreven staat valt al onder het beroepsgeheim.

RS: Ja, want op wat voor manier steekt de gemeente dat in dan? Waarom hebben zij die informatie nodig?

Zorginstelling D: Nou ja, zij zien dat als uitvloeisel van de wettelijke opdracht die zij hebben gekregen om in het sociale domein voorzieningen te treffen en daar zorg te verlenen, maar zorg gaat veel verder dan de geneeskundige zorg en wij zitten met die individuele geneeskundige zorg binnen het medisch beroepsgeheim, maar degenen die meer algemene voorzieningen doen, die hebben natuurlijk ook wel te maken met privacy, maar die kunnen dat nog iets ruimer opvatten dan binnen medisch beroepsgeheim.

RS: Ja, nou zie je natuurlijk ook bij gemeentes genoeg misgaan wat dit onderwerp betreft.

Zorginstelling D: Nou ja en dat stelt ons natuurlijk helemaal niet gerust als je denkt aan hoe moeilijk het is in zo'n organisatie als dit om dat dicht te timmeren, terwijl er over het algemeen best wel veel bewustzijn bij mensen is denk ik dat je niet wilt dat er een psychiatrische geschiedenis op straat ligt, ja dan maak ik me wel eens zorgen hoe gaat dat bij de gemeentes?

RS: Ja, daar komt natuurlijk ook een heleboel informatie binnen en op wat voor manier steken jullie die voorlichting dan in? Is daar al een idee over? Gaat dat met presentaties of?

Zorginstelling D: Nou we hebben een intranet dat is altijd een belangrijk medium voor nieuwsberichten. We hebben ook een intern magazine dat met enige regelmaat uitkomt dus daar kun je dingen inzetten. En ja verder kan ik wel gaan fantaseren maar hebben we het niet uitgewerkt, dus wat dat betreft ben je net iets te vroeg omdat we nu nog eigenlijk ik en het hoofd informatiemanagement zijn nu communicatie aan het voeden met informatie en zij komen dan met een plan.

RS: Ja, ja precies, dus op dit moment hebben medewerkers eigenlijk toegang tot dat systeem en daar staan de regels wel in maar voor de rest moet nog komen zeg maar?

Zorginstelling D: Nee, zeg maar het meer push met posters of nou ja via nieuwsberichten etcetera dat moet nog. Maar dan verschijnt altijd de voorste pagina van het intranet en daar staan ook de nieuwsberichten op en van daaruit kun je doorklikken naar de patiëntendossiers of naar de documenten.

RS: Ja, precies. En wanneer zijn jullie van plan met die campagne te beginnen?

Zorginstelling D: Uhm, wat hadden we afgesproken? Ja er was één aspect dat wilden we nog dit jaar starten, dat was die datalekken, daarbij hadden we echt zoiets van dat willen we zo snel mogelijk doen.

RS: Ja want is er op dit moment al iets van een meldpunt voor medewerkers waar ze…?

Zorginstelling D: Nou ja het staat nu wel in het privacydocument dat je een datalek moet melden bij de functionaris gegevensbescherming, dus dat ben ik. Maar goed we willen nog zowel in de campagne als in een apart schemaatje dat nog wat versimpelen zeg maar.

RS: Ja, want de medewerkers werken wel allemaal in deze ruimte of zijn er ook heel veel mensen die misschien op andere plekken werken?

Zorginstelling D: Nee, dat is in de communicatie altijd lastig we hebben een enorm groot gebied, dus het is een hele grote regio met geloof 60 locaties of zoiets. En ja je moet dus mensen, je kunt ze niet allemaal persoonlijk benaderen. Je kunt niet zeggen van goh nou nu gaan we een middag organiseren en dan komt iedereen dat lukt niet. Dat is natuurlijk sowieso al moeilijk in de zorg, maar het zal dus toch vooral via elektronische weg moeten of papier. Ja, daar blijf je ook deels afhankelijk van ja is er de wil van mensen om het tot zich te nemen, want niet iedereen staat op dezelfde manier in z'n werk hè sommige mensen denken ook ik doe m'n werk en ik ga weer naar huis, klaar. Dus ja dan kun je het bijna onder de neus wrijven, maar he ik vind even vanuit de werkgever geredeneerd wij zijn verplicht om mensen zo goed mogelijk voor te lichten en ja als mensen dingen dan vervolgens niet goed doen dan kun je in ieder geval nog zeggen ja we hebben wel ons best gedaan om mensen dat bij te brengen, erop te wijzen dus ja werknemers hebben daar uiteindelijk ook een eigen verantwoordelijkheid in.

RS: Ja, een eigen rol in en zijn er op dit moment al maatregelen bijvoorbeeld voor werknemers als ze zich niet aan regels houden?

Zorginstelling D: Nou nog niet expliciet en daar moet, dat is ook wat ik zei één van de aspecten het sanctiebeleid laten we maar zeggen, dat moet duidelijker omschreven worden. Er zijn wel incidenten geweest dat mensen onrechtmatig in dossiers keken en dat dat natuurlijk bekend werd toen. Ja in één geval heeft dat geleid tot ontslag en in een ander geval tot een ernstige waarschuwing. En dan zie je dat omstandigheden net wat anders waren, waarbij je bij de één zegt ja daar was eigenlijk al een keer voor gewaarschuwd, maar dan is het gewoon via de algemene regels, arbeidswetregels worden dingen afgehandeld, maar mensen hebben natuurlijk eigenlijk wel recht om dat van tevoren te weten nou als je dat doet dan loop je dit en dit risico.

RS: Ja, ja, precies, want zijn er dan ook bijvoorbeeld gedragscodes binnen deze instelling?

Zorginstelling D: Uh, dat is een goede vraag. Ja, maar die gaan niet zover als op dit. Dat gaat veel meer over gedrag en hoe je met elkaar omgaat.

RS: Oké dus niet gericht op privacy?

Zorginstelling D: Nou kijk, mijn twijfel is natuurlijk meteen als er gedragscodes zouden zijn dan zou ik ze moeten kennen, maar vraag mij niet. Ik weet dat er oneindige discussies zijn geweest over gedragscodes en nou ja iedereen vindt daar wat van. Als je me nu zegt van welke zijn het, geen idee.

RS: Nee, ja maar dat is ook als je een willekeurig iemand vraagt wat zijn de privacyregels hier dan kunnen ze die waarschijnlijk ook niet zo opzeggen, dat moet je toch altijd opzoeken met dat soort dingen.

Zorginstelling D: Maar ik denk dat er in de psychiatrie zeker en misschien in de zorg in z'n algemeen ook wel een bewustwording is dat mensen snappen dat je informatie niet op straat legt.

RS: Nee, dat kan ik me ook voorstellen inderdaad, want in hoeverre denk je dan dat communicatie een rol zou kunnen spelen in het inperken van de risico's die je loopt?

Zorginstelling D: Ja, dat is denk ik heel erg belangrijk omdat de regels ook aangescherpt zijn en ja zeg maar toch het naar voren brengen van dit aspect. Kijk het lastige is in zo'n zorgorganisatie zijn zoveel aspecten waarover mensen geïnformeerd moeten worden dat je als organisatie ook keuzes moet maken van waar leggen we nu de nadruk op? De zorg verandert steeds ook de regels veranderen steeds en overal moeten mensen over

geïnformeerd worden en alles lijkt belangrijk als je er mee bezig bent en medewerkers worden echt overvoerd met informatie, die worden daar helemaal gek van van 'goh heb je dit weer dan heb je dat weer'.

RS: Hoe worden die keuzes daar dan in gemaakt? Worden die door communicatie gemaakt of door de Raad van Bestuur?

Zorginstelling D: Ja, communicatie in samenspraak met de Raad van Bestuur maar soms ook de waan van de dag, zo'n datalekwet die er dan ineens komt die financiële risico's met zich meebrengt.

RS: Ja en natuurlijk heel veel aandacht in de media.

Zorginstelling D: Ja, veel te veel vind ik ook hoor, want ik merk dat de regelgeving eigenlijk heel onduidelijk is, eigenlijk weten we niet wat we wel en niet moeten melden en dan zie je omdat er in theorie zo'n hele grote boete tegenover staat dat we dus alles melden. Laatst was iemand, was er een ID-kaart gestolen van een patiënt, ja dat heb je dan maar gemeld, want ja als je de regels nagaat dan moet je dat melden hè, het zijn bijzondere gegevens want het zijn patiëntgegevens BSN-gegevens, ja moet je melden, maar ik geloof zelf nooit dat die wet daarvoor bedoeld is, die wet was veel meer bedoeld voor grote inbreuken.

RS: Ja, je hebt natuurlijk ook bijvoorbeeld hackers die in kunnen breken.

Zorginstelling D: Ja nou precies of iemand die zijn usb ergens laat liggen of een laptop wordt gekraakt.

RS: Ja, want hoe gaan jullie daarmee om met laptops, usb-sticks? Is daar beleid voor?

Zorginstelling D: Ja, daar is in zoverre beleid voor het systeem laat het ook niet toe om usb-sticks te kopiëren maar er is natuurlijk altijd de omweg dat je iets kunt e-mailen naar je eigen adres en dan op een usb-stickje kunt zetten. We hebben toevallig ook vorig jaar een verbeteractie gehad met de ja mensen die hier onderzoek doen, wetenschappelijk onderzoek vanuit de opleiding. We hadden wel SPSS losse versies, maar die stonden dus op laptops die mensen dan meenamen en dat vonden we wel een risico en mensen vonden het zelf dan ook wel weer lastig, dus die gingen dan vaak gegevens overhevelen naar de universiteitsserver dan konden ze daar op SPSS werken. Nou ja dat hebben we verbeterd door een netwerkversie aan te schaffen, waarin mensen die wetenschappelijk onderzoek doen dus via het netwerk op SPSS terecht kunnen. Dus niet meer extern hoeven te doen, ook niet thuis, want je kunt dus ook thuis inloggen op het systeem.

RS: Ja, want je kunt dus wel overal inloggen ook via je laptop?

Zorginstelling D: Ja, je kunt overal op de wereld in principe inloggen in het systeem. Dat is beveiligd en dan zit je gewoon binnen het beveiligde systeem van onze instelling en daar heb je natuurlijk meer mogelijkheden en daarbij is ook een protocol geschreven voor het anonimiseren van gegevens van hoe doe je dat en dus wanneer vinden wij dat het geen persoonsgegevens meer zijn.

RS: Want SPSS ik kan me zo voorstellen normaliter als je onderzoek doet dan staan daar geen persoonsgegevens in.

Zorginstelling D: Nee maar wat je hier natuurlijk soms hebt is dat mensen gegevens willen hebben, maar die komen natuurlijk uit een patiëntenbestand en die moeten geanonimiseerd worden en niet iedereen die deed dat op dezelfde manier en af en toe kon je gewoon het ene met het andere nummer weer combineren en dan wist je precies wie het was, ja als ze bijvoorbeeld het patiëntennummer laten staan bijvoorbeeld.

RS: Ah op die manier. Dus dat is onderzoek onder patiënten.

Zorginstelling D: Ja, het meeste onderzoek is hier natuurlijk onder patiënten en dat is al één ding want dat moet dan natuurlijk uit databases gehaald worden en dat dan die dingen zo geanonimiseerd worden en soms deden ze dat ook pas als ze die dingen al thuis hadden staan. En daar hebben we afspraken over gemaakt van hoe dat anders moet.

RS: Ja, oké en is hier dan ook verandering in na de Meldplicht Datalekken dat hier meer aandacht voor is ook in deze organisatie?

Zorginstelling D: Nou, op bestuurlijk niveau is er wel heel veel aandacht voor geweest. Ik heb natuurlijk zelf heel veel vragen gekregen als jurist 'joh waar staan we en wat zijn onze risico's?' Dus daarom is ook die functie van FG ontwikkeld, maar in de organisatie zelf is daar nog niet zo heel veel aandacht voor geweest. Ja, ik heb wel eens een keer een nieuwsberichtje over het feit dat er een FG is en wat dat dan betekent geschreven, maar ja dat is één berichtje en een week later is het weg en dan zullen mensen het weer vergeten zijn. Het is wel opvallend dat wanneer je zo'n bericht neerzet dat je dus die week ontzettend veel vragen en meldingen krijgt op iets.

RS: Oké ja want hoe gaat het hier met de meldingen, komen er veel binnen?

Zorginstelling D: Ik heb nu drie meldingen gedaan bij de Autoriteit Persoonsgegevens. Toevallig kwamen er twee weken geleden twee in één week, maar ik denk dat dat een enorme onderregistratie is. Omdat je omdat we er toch voor kiezen om ook de kleine incidenten te melden, dus hè als iemand een e-mail naar het verkeerde adres stuurt, ja dan heb je eigenlijk al een datalek hè als daar nog persoonsgegevens in staan.

RS: Ja, is officieel wel zo natuurlijk.

Zorginstelling D: Ja, wat dat betreft, maar dat was nog voor de wet datalekken, hadden we ook wel een mooi, of nou ja een mooi incident, ook voor dat mensen vragenlijsten moeten invullen voordat ze in zorg komen en sommige mensen hebben geen e-mailadres en dan moest het in het softwaresysteem moest iets ingevuld worden en daar hadden ze ook een afspraak over gemaakt wat je in moest vullen, maar ergens op het secretariaat hadden ze bedacht we bedenken zelf wel even een e-mailadres. En dan bleek dus het vervelende te zijn dat dat een bestaand e-mailadres was en dat kwam dus bij een bedrijf terecht en ja die man kreeg dus in één keer allerlei mailtjes en daar stond dus wel de naam en geboortedatum van iemand in dus ja dat was ja daar ging natuurlijk van alles mis, want ja die mailtjes van die man die bleven ergens in de postbus haken wat niemand zag enzo dus die man werd op een bepaald moment boos. Zo van, als jullie nou niet stoppen dan ga ik naar de pers en dat soort dingen en dat is dus wat je echt niet wilt, ja maar goed. Toen hoefden we dat nog niet te melden dus toen hebben we het wel gecorrigeerd en die man onze excuses aangeboden, maar ja hij heeft ook gezegd ik heb dat allemaal vernietigd en weggegooid ja dat moet je dan maar hopen.

RS: Ja, daar moet je dan maar in geloven. Je kunt niet mensen gaan dwingen om dingen weg te gooien, ja dat is natuurlijk zo. En als er dan zo'n datalek gemeld wordt dan komt dat bij jou binnen. Kunnen medewerkers dat gewoon anoniem doen of doen ze dat meestal bij naam?

Zorginstelling D: Eigenlijk is het de bedoeling dat ze twee dingen doen: we hebben een incident-meldsysteem en daar kun je ook beveiligingslekken melden, dus het moet in dat systeem gedaan worden. Dat zou ik dan kunnen zien, maar ja de praktijk is dat die mailtjes niet altijd zomaar. En je moet binnen 72 uur eigenlijk reageren hè. Dus het idee is eigenlijk dat als iemand iets kwijt is geraakt dat diegene dat meldt bij zijn leidinggevende en dat de leidinggevende het meldt bij mij. Ja, we hebben het niet over anoniem melden gehad, ja dat is ook heel erg lastig want je hebt informatie nodig van ja wat is er gebeurd? Heb je het verteld aan degene die het betreft? Kijk en het idee van incidenten melden is natuurlijk dat dat niet leidt tot sancties, tenminste niet het melden zelf.

RS: Nee, nee precies.

Zorginstelling D: Dus je probeert vooral te onderzoeken van hoe kunnen we voorkomen dat het weer gebeurt?

RS: Ja, ja, en hoe maak je medewerkers dan daarop attent? Want ik kan me voorstellen natuurlijk dat medewerkers denken nou ik meld iets liever niet want misschien krijg ik wel op mijn dak. Hoe motiveer je die mensen om wel meldingen te gaan doen?

Zorginstelling D: Ja, ja, kijk dat systeem geldt ook voor agressie en dat soort zaken en mensen kennen het systeem wel goed dus hoe je moet melden en er is op zich wel een redelijk grote meldingsbereidheid, maar ja ik weet natuurlijk niet wat mensen niet melden, dat weet ik ook niet. Maar ik kan me voorstellen dat met een datalek de drempel wel wat hoger is. Laatst was iemand bijvoorbeeld een testrapport kwijtgeraakt als psycholoog tijdens een verhuizing was dus nog op papier, ja de doos moest van het ene naar het andere gebouw dat is netjes gebeurd, die doos is wel overgekomen alleen het rapport is in die tijd, er zat ook nog een vakantie tussenin, toen ze de doos uitpakte was het rapport weg. Ja, toen is ze een week lang is ze aan het zoeken geweest naar dat rapport totdat ze echt dat ja ik kan het echt niet vinden en toen is ze naar haar leidinggevende gegaan van ja ik ben het kwijt. En toen was die leidinggevende chagrijnig zo van ja waarom vertel je me dat nu pas een week nadat je dat geconstateerd hebt? Ja, anderzijds kan ik het me ook wel voorstellen want ja het is natuurlijk erg lullig dat het gebeurt dus je probeert natuurlijk alles in het werk te stellen om dat ding terug te vinden en dat je op een bepaald moment dan die drempel op gaat van ja ik moet het dan toch maar melden.

RS: Het is eigenlijk een beetje vergelijkbaar met als je je portemonnee kwijtraakt of iets dergelijks dan hoop je in eerste instantie ook nog dat je hem terugvindt.

Zorginstelling D: Ja, deels lijkt het daar op, maar het is natuurlijk ook gênant om dat te moeten melden. Ik denk dat het ook gênant is: stel je voor je hebt toch gegevens naar je privéaccount verplaatst want je wilt thuis er nog aan werken, dat is op zich een oprechte reden en je computer of je laptop wordt gestolen of gehackt ja dan moet je denk ik wel even een drempel over om dat te zeggen, omdat je dan inderdaad ook toe moet geven dat je iets gedaan hebt wat niet mag. Dus dat blijft een moeilijkheid. Het zit natuurlijk wel als die gegevens op straat komen en blijkt dat je het dan wist en je hebt het niet gemeld dan heb je natuurlijk ook een probleem.

RS: Ja, een groter probleem misschien wel, want je hebt natuurlijk bij jullie ook wel kwaliteitsmeldingen dus daar weten mensen al wel vanaf dat ze dingen moeten melden.

Zorginstelling D: Ja, ja dat zei ik dat systeem waarop je agressiemeldingen of valincidenten doet. Dat zit in één systeem en je kunt gewoon kiezen wat voor soort melding je doet, dus dat systeem kent men wel.

RS: ja, dus daar hoeven ze in ieder geval niet meer in getraind te worden.

Zorginstelling D: Nee, daar zijn in het verleden campagnes op geweest en dat werkt.

RS: En hoe werden die campagnes toen bijvoorbeeld ingestoken? Wat werd toen gedaan?

Zorginstelling D: Oeh, dat is alweer een paar jaar geleden. Uhm, ja eigenlijk wel dezelfde kanalen als die ik zonet noemde. Dat was dus via intranet, maar ook naar managementoverleggen gaan waar mensen met het team dan zitten. Je hebt vaak wel één keer in de veertien dagen ofzo werkoverleg dat je je daar laat uitnodigen en dan uitlegt van joh dit systeem is er en wil je medewerkers daarop wijzen dat ze dit systeem gaan gebruiken.

RS: Ja, dus eigenlijk van bovenaf een beetje naar de organisatie toe.

Zorginstelling D: Ja en je zit ondertussen er wel een beetje mee dat wanneer het gaat om incidenten melden dat het geregionaliseerd is hè dus er zijn nu mensen op locatie die meldingen afhandelen. In het begin ging dat allemaal heel erg centraal en nu is er de gedachte, ja als er een incident is dan moet je dat vooral op de afdeling waar het gebeurd is in eerste instantie afhandelen. Dus er zijn daar ook nu mensen die daar bewust mee bezig zijn en hopelijk ook collega's daarop wijzen.

RS: Ja, het is misschien ook een iets minder grote stap om te melden aan je directe leidinggevende dan dat je meteen voor een datalek bij jou terechtkomt.

Zorginstelling D: Nou ja, wat je ziet is hè af en toe gebeurt er een incident of een calamiteit. Dat waar dat gebeurd is, is er altijd een enorme awareness bij zo'n afdeling en dan hoef je niemand meer voor te lichten, die mensen weten het allemaal precies. Alleen hoe draag je dat dan over naar de rest van de organisatie en dat is

moeilijk. En ik verwijt ons ook wel dat we niet echt een hele goede lerende organisatie zijn. Ja, dat is niet bewust, maar om nou te gaan zeggen van 'ja goh let erop want daar en daar is dit misgegaan'. Dat is toch een beetje als je vuile was buiten hangen.

RS: Ja, dus er worden geen casussen besproken of iets dergelijks?

Zorginstelling D: Nee, als er een groot onderzoek is geweest omdat er een calamiteit is geweest. Dat komt niet op intranet van goh dit zijn de bevindingen geweest en dit zijn de verbetermaatregelen en hé jongens wil iedereen daar even op letten, terwijl dat in mijn ogen wel goed zou zijn om dat wel te doen. Je moet natuurlijk altijd oppassen dat je ook niet de privacy van de medewerkers schendt en dat soort zaken, maar ja met een beetje goede wil.

RS: Ja, daar zijn natuurlijk mogelijkheden voor.

Zorginstelling D: Maar ik denk dat er toch angst is dat zo'n bericht ook als je dat intern doet dat dat ook naar buiten gaat.

RS: Ja, in de media terechtkomt.

Zorginstelling D: Ja, zoals wat gisteren met zo'n verpleeghuis was hè zo'n plascontract.

RS: Oh dat heb ik niet meegekregen gisteren.

Zorginstelling D: Ja, er kwam in het nieuws dat wanneer mensen in een verpleeghuis kwamen dat mensen dan iets moesten ondertekenen dat ze drie keer per dag mochten plassen.

RS: oké.

Zorginstelling D: En dat lijkt natuurlijk heel erg ernstig, maar gisteravond toen werd dat door de directeur van dat verpleeghuis ook wel heel erg genuanceerd van nou ja dit is helemaal uit zijn context gehaald en daar zie je dus dat voor je het weet tegenwoordig met moderne media dat als iets niet goed is je er heel weinig greep op houdt om dat nog te corrigeren.

RS: Ja, maar wat was dit dan voor verhaal? Er was iets naar buiten gekomen waarop stond welke mensen wanneer naar de wc gingen?

Zorginstelling D: Zeg maar een soort zorgplan waarin dan stond van u mag drie keer per dag naar de wc ofzo. Ik heb de discussie ook niet helemaal gevolgd, maar dat lijkt natuurlijk bizar dat als je in een verpleeghuis wordt opgenomen dat je dat moet ondertekenen. Zo werd dat een beetje gebracht van nou je moet eerst dat ondertekenen…

RS: en dan mag je pas naar de WC.

Zorginstelling D: Ja dan mag je pas in het verpleeghuis komen, nah dat bleek allemaal veel genuanceerder dat ging erom dat je op een gegeven moment wel wat structuur moet aanbrengen in de dag, er zullen soms dementerenden wel 36 keer per dag naar de wc moeten, maar dit was niet zoals het is gebracht. Ondertussen dan reageert de minister al en dat is natuurlijk ook de angst voor een organisatie als dit van als er dingen op straat liggen, ja dat heb je niet meer onder controle. De nuancering raakt heel snel kwijt. We hebben ook wel incidenten gehad waar mensen naar de televisie gingen en bij de EO op de vijfde dag ofzo kwam het en dan denk je soms ook van ja dat gaat wel heel erg ongenuanceerd en daar ben je dan natuurlijk niet zo blij mee als dat zo is. Anderzijds zijn we er ons als organisatie ook wel heel erg van bewust dat transparantie de norm is tegenwoordig, je moet gewoon heel erg transparant zijn. Tegenwoordig als we calamiteitenplannen opstellen dan zullen we dat altijd delen met betrokkenen en familie en dat ja als de familie ermee naar de pers stapt dan tsja dat is dan maar zo.

RS: Ja, dat zie je overal natuurlijk. Je ziet het bij gemeenten, je ziet het bij scholen. Sommige dingen worden helemaal landelijk overgenomen in het nieuws.

Zorginstelling D: Ja dan zie je toch een soort dynamiek.

RS: Ja, je kan er niks meer aan doen als organisatie, alle mensen staan op de stoep.

Zorginstelling D: Nee, maar daar hoop je dan inderdaad op dat er ergens in de wereld iets heel ergs gebeurt. Maar wat ik wel echt een probleem vind is wat jij net zelf ook zei: het kan iets doen met de bereidheid van mensen om eerlijk te vertellen wat er gebeurd is. Mensen wordt gevraagd in zo'n onderzoek, vertel wat er gebeurd is het is niet bedoeld om je daarna een tik op de vingers te geven maar om ervan te leren hè hoe kunnen we dit nou in de toekomst voorkomen. Maar als mensen weten dat het straks op straat ligt, dan heb je het risico dat mensen toch terughoudender worden hè. Je wilt ook niet straks van journalisten een microfoon onder je neus krijgen.

RS: Nee, ja want denk je dat buiten jouw functie privacy in jullie organisatie een hoge prioriteit heeft of een lage?

Zorginstelling D: Ja, vind ik wel. Nee, het heeft hoge prioriteit. Natuurlijk vinden allerlei slordigheden plaats, dingen waarvan je denkt dat kan beter niet. Maar ja wij hebben zo'n 20.000 patiënten per jaar en als je dan kijkt naar het aantal incidenten die in ieder geval bij mij bekend worden dan is dat niet veel. Dan denk ik van nou met 2400 medewerkers. Het leidt niet heel vaak tot ernstige incidenten waarvan je echt denkt van nou dit is echt heel erg.

RS: Nee, maar het kan natuurlijk ook zijn dat mensen het niet melden.

Zorginstelling D: Nee, daar ben ik me absoluut van bewust dat heel veel niet gemeld wordt de kleine dingen, maar dan is blijkbaar degene die het betrof of het heeft niet geleid tot iets of degene die het betrof heeft ook zelf gezegd van nou ja kan gebeuren, want dat is natuurlijk ook wel heel vaak zo.

RS: Ja, want je hebt dan nu in totaal drie keer een melding gedaan bij de Autoriteit Persoonsgegevens en ja heb je van hen ook informatie ontvangen hierover?

Zorginstelling D: Nou nee dat is dus de hele droefheid ervan. Ja, dat vind ik wel, want het roept op dat je in een enorm bureaucratisch systeem terecht bent gekomen. Je hoort echt helemaal niets terug, niet eens een ontvangstbevestiging. Ja je moet het formuliertje invullen en dan staat er van u heeft het ingevuld, bedankt.

RS: Je krijgt geen mail of iets dergelijks van bevestiging?

Zorginstelling D: Nee en ook niet van kans op onderzoek ofzo of wat dan ook. Een tijdje geleden hoorde ik ook dat ze vorig jaar 60.000 meldingen hadden gehad, ja daar kunnen ze natuurlijk ook helemaal niks mee.

RS: 60.000? Maar ze zitten nu pas op…

Zorginstelling D: Nou ja vanaf 1 januari is dat dan hè

RS: Ja, maar ze zitten nu pas op 4000 of iets dergelijks.

Zorginstelling D: Is dat zo?

RS: Ja, dus dat vind ik wel een bijzonder aantal 60.000. Maar misschien zijn dat ook algemene? Niet alleen Meldplicht Datalekken. Bij Meldplicht Datalekken zaten ze in ieder geval twee week terug op iets van 4000 meldingen.

Zorginstelling D: Oh, nou dan heb ik een verkeerd getal. Maar dan nog ook op 4000, ja wat moeten ze ermee? En dan krijgen ze dat soort flutmeldingen die ik dan doe, waarvan ik ook denk ja daar willen ze ook helemaal niks mee denk ik.

RS: Ja, want hoe kijk je dan tegen die rol aan van de autoriteit?

Zorginstelling D: Ja, ja, wat moet ik daarvan vinden? Kijk, als ik zelf denk ook waar volgens mij de regels op gedoeld zijn dat zijn meer de grotere incidenten en dat ze daar een rol in vervullen dat lijkt me heel goed, maar dit heeft niet zo heel veel effect op de kleinere incidenten dan denk ik van ja. Ik vind het ook lastig dat die regelgeving in die zin onduidelijk is. Aan de ene kant hele hoge boetes en aan de andere kant een onduidelijke regelgeving, ja…

RS: Ja, want ben je wel eens naar hen toegestapt met vragen hierover?

Zorginstelling D: Nee, ik volg meer de landelijke discussie hierover en als je kijkt GGZ-Nederland heeft wel zo'n website waar je onderling aan elkaar vragen kunt stellen. Ja, iedereen heeft die vraag wat moet je wel of niet melden? De meeste instellingen kiezen er dan maar voor om het zekere voor het onzekere te nemen, want op zich zo'n formuliertje invullen dat is het werk niet, een kwartiertje.

RS: Oh, ik vind dat vrij uitgebreide formulieren volgens mij heb je een boel informatie nodig.

Zorginstelling D: Nou ik vind het wel meevallen hoor. Het is toch van nou wat is er gebeurd en wat heb je vervolgens gedaan. De moeilijkheid in het systeem is dat je kunt een voorlopige melding doen, maar als je hem dan vervolgens weer oproept, moet je gewoon weer het hele formulier opnieuw invullen, je krijgt niet je oude formulier terug.

RS: Ja, dat heb ik ook inderdaad begrepen. Ik ben naar een bijeenkomst geweest van NVFG, Nederlands Vakgenootschap voor Functionarissen Gegevensbescherming, ik weet niet of je daarbij aangesloten bent. Maar die hadden een Ronde Tafelbijeenkomst en toen was de Autoriteit Persoonsgegevens die was daar ook, ja toen kwamen er natuurlijk ook een boel vragen uit de zaal van hoe zit dit en hoe zit dat. Ik zat daar met het idee dat daar praktijkcasussen besproken zouden worden, maar dat was niet echt het geval. Ja, iedereen was redelijk terughoudend in het noemen van waar ze vandaan kwamen. Het ging heel erg algemeen in op de wet.

Zorginstelling D: Ja, wat ik gezien heb toen deze wet eraan zat te komen dat ook vanuit commerciële hoek de angst enorm vergroot is. Er zijn echt advocatenkantoren en andere kantoren geweest die met name op bestuurlijk niveau enorm de angst gevoed hebben. Pas op, als jullie het niet op orde hebben dan… En let u wel even op uw persoonlijke bestuurlijke aansprakelijkheid hierin en ja het was allemaal niet gelogen maar het was ook toch wel veel bangmakerij om toch werk te krijgen vond ik hoor. Zo van als jullie je bewerkersovereenkomsten niet op orde hebben dan… En dat is heel specialistisch werk, terwijl er ondertussen al standaard bewerkingsovereenkomsten circuleerden die ja, voor 90% gewoon goed zijn en dan moet je nog een paar dingetjes voor je persoonlijke aanpassen.

RS: Ja, ja precies.

Zorginstelling D: Ja, dus ik heb wat dat betreft ook meer moeite gehad de directie hier gerust te stellen zo van ja dat valt allemaal wel mee.

RS: Ja, de Autoriteit Persoonsgegevens heeft natuurlijk tot dusver ook nog geen boetes uitgedeeld.

Zorginstelling D: Nee, en ze hebben het op een bepaald moment ook wel wat genuanceerd hè dat ze niet in één keer een factuur schrijven, maar dat ze waarschuwen.

RS: Kunnen ze ook niet gaan doen denk ik, want ja gaan ze dat doen: hoe meer boetes zij gaan uitdelen, hoe minder mensen gaan melden.

Zorginstelling D: Nou ja je wordt natuurlijk beboet als je niet meldt hè?

RS: Ja, ja, ja. Maar als je dan wel iets meldt maar er blijkt achteraf bijvoorbeeld dat je niet genoeg stappen hebt genomen of je medewerkers hebben totaal geen bewustzijn hiervoor er is niks van een campagne geweest dan kom je ook in de problemen terecht.

Zorginstelling D: Ja, daarom. Maar in die zin, laatst hoorde ik iemand in een interview ook op de radio zeggen ja het wordt tijd dat er een keer een boete wordt uitgeschreven. Ja, ik denk, ja dat is een politiek middel dan.

RS: Ja, het is natuurlijk wel zo dat tenminste ik hoor ook vaak vanuit de privacyhoek ja wij willen wel dat er een boete komt, want er zijn natuurlijk ook heel veel instellingen waar dit thema nog geen hoge prioriteit heeft, waarvan mensen wel willen dat het een hoge prioriteit krijgt. Ja, als er boetes komen dan krijg je automatisch natuurlijk wel meer prioriteit in de organisatie want dan kunnen ze daadwerkelijk schade oplopen.

Zorginstelling D: Nou ja je loopt nu wel het risico dat omdat het zo fors gebracht is ook door marktpartijen van pas op die boetes, dat iedereen heeft even op scherp gestaan dat als er nu niets gebeurt, twee jaar lang ofzo, ja dan zakt het ook weer in, omdat organisaties zich daarop aanpassen. Er zijn natuurlijk veel meer toezichthouders en ja als je het idee hebt van ze zijn er wel maar ze doen toch niks. Wij moeten ook bij de AP melden welke persoonsgegevens wij verwerken en op welke plek nou dan heb ik eens even gekeken wat wij daar hebben staan dat is volgens mij van 20 jaar geleden ofzo, dat is enorm verouderd, maar daar gebeurt dus ook niets mee en dan kijk ik bij andere instellingen en dan wij hebben er nog vier of vijf dingen staan en anderen hebben er maar één of twee dingen staan. Er is dus ook geen enkele controle vanuit de autoriteit om te zeggen van 'goh wat jullie daar hebben klopt dat wel?'

RS: Nee, hebben ze misschien ook geen capaciteit voor.

Zorginstelling D: Dat denk ik ook niet. Ik weet niet hoeveel mensen daar zitten.

RS: Ja, best weinig. Die kunnen nooit al die meldingen doornemen en het zijn er nu nog heel weinig voor de verhouding van wat je mag verwachten dat er gemeld wordt.

Zorginstelling D: Nee, ik denk dat dat fors toeneemt. Laatst hoorde ik een instelling die hadden een lijstje met patiëntnamen was op de printer blijven liggen en dat was daar een uur of twee uur blijven liggen en toen werd ie weer gevonden en dat was in een publieke ruimte geweest en toen hebben ze het toch gemeld ook al lag die nog gewoon op het kopieerapparaat van ja in theorie kan het zo zijn dat iemand dat papiertje gepakt heeft door de printer gedaan heeft en een kopie meegenomen heeft. Ja, als je dit soort dingen, strikt genomen moet je het melden, maar daar zit volgens mij niemand op te wachten.

RS: Nee, nou ja, je hebt natuurlijk nu eigenlijk een soort tussenperiode want we gaan natuurlijk uiteindelijk naar de Europese Verordening toe in 2018, die is nu geloof ik heb ik begrepen al wel van kracht maar wordt nog niet gehandhaafd. In hoeverre denk je dat jullie daar op voorbereid zijn?

Zorginstelling D: Ja daar zijn we op dit moment wel hard mee bezig. Ik bedoel met die externe partij aan het kijken in hoeverre voldoen we daaraan, maar dat zit met name rond de bewustwording, toezicht en sanctiebeleid.

RS: Ja, dat kwam dan uit die nulmeting?

Zorginstelling D: Dat kwam dus uit die nulmeting en nu moeten we wat meer concreet gaan kijken van welke punten schieten we nu tekort en ja dan moet je gaan prioriteren waar je als eerste mee aan de slag gaat.

RS: Ja en die nulmeting die is gedaan in januari ergens begin dit jaar?

Zorginstelling D: Nee, iets later, mei geloof ik.

RS: Dus die is toen gedaan en nu is er eigenlijk dus stap 2 waar gaan we…

Zorginstelling D: Ja, dan ga je weer iets meer de diepte in dus nu gaan we iets meer kijken van goh waar moeten we nog een verbeterslag maken.

RS: Nee, oké duidelijk. Ik denk dat ik alle informatie heb hierover. Ja, even kijken of ik nog dingen mis. Altijd even handig om te kijken, ik moet natuurlijk wel allemaal een beetje dezelfde lijn aanhouden anders kun je natuurlijk niks met elkaar vergelijken. Even kijken, ja ik heb alle dingen besproken. Heel erg bedankt voor de medewerking.

5.5 Uitwerking interview zorginstelling E

RS: Eerst benieuwd vanuit welke weg ben je op deze positie terechtgekomen? Het is natuurlijk vrij nieuw de functie van functionaris van de gegevensbescherming, privacy officer.

Zorginstelling E: Ja, klopt. Ik werk sinds 2010 hier. Ik begon als senior systeembeheerder. Na 2 jaar ben ik ICT-architect geworden. Toen heb ik me beziggehouden met vooral de inrichting van het applicatie en informatielandschap. En ja dan dien je dus ook rekening te houden met allemaal kaders die er zijn en dat heeft automatisch ook een technisch karakter, maar ik ben altijd nieuwsgierig geweest. Zodoende kwam ik ook achter de Wet Meldplicht Datalekken en dat het eraan zat te komen en toen heb ik dat al besproken, onder de aandacht gebracht wat hogerop, dus bij de bestuursstaf en zodoende is eigenlijk vanuit de bestuursstaf de wens uitgesproken van waarom ga jij niet functionaris van de gegevensbescherming worden? Dus daar heb ik even over na moeten denken en toen gezegd van ‘nou laten we dat maar doen’. De functie is nodig en het is goed als we hier een dergelijke functie hebben, dus laat ik hem maar gaan vervullen. Dus eigenlijk sinds begin dit jaar ben ik hier functionaris.

RS: Sinds de wet ook is ingetreden?

Zorginstelling E: Ja, sinds de wet in werking is getreden of eigenlijk sinds februari.

RS: En volg je daar ook een opleiding voor?

Zorginstelling E: Die volg ik. Een opleiding van twee jaar. Alle aspecten die bij een functie komen kijken die worden daar behandeld. Je hebt natuurlijk een stuk wetgeving, maar ook governance en ook de technische infrastructuur, maatregelen worden besproken, maar het wordt ook in perspectief van Europa gezet of als je eventueel met internationale ondernemingen gaat samenwerken. Een vrij brede opleiding vind ik en erg interessant.

RS: En je zei al over het bestuur dat je het daar eigenlijk onder de aandacht hebt gebracht. Hoe zien zij dit? Hoe hebben zij dit in beeld dit thema?

Zorginstelling E: Nou ik heb in eerste instantie met de bestuursstaf gesproken en dat is eigenlijk via het informele circuit. Ik werk hier al een tijdje dus ik ken veel mensen, dus dan weet je gewoon voor dit onderwerp moet ik bij die zijn, dus ben ik gewoon maar even een kop koffie gaan drinken en ben ik gaan praten gewoon en dat is dus bij de bestuursstaf terechtgekomen en daar kwamen we tot de conclusie van ja dit moet niet een losstaand initiatief zijn het moet gedragen worden vanuit het bestuur alleen dan kun je er eigenlijk voor zorgen dat je voldoende maatregelen kunt treffen als organisatie. Het is niet alleen een technisch stuk, maar ook een organisatorisch stuk en je hebt daar gewoon het support en het mandaat ook wel van het bestuur voor nodig. Dus om je vraag te beantwoorden het bestuur die staat daar helemaal achter. Daar hebben we ook mee aan tafel gezeten en helemaal uitgelegd wat we willen. Ik heb een plan van aanpak geschreven voor een periode van twee jaar waarin ik aangeef hoe we gaan werken aan het organiseren van gegevensbescherming binnen deze organisatie.

RS: Ja, dus dat plan dat werd vanuit jou beschreven en dan werd het bijvoorbeeld door het bestuur goedgekeurd.

Zorginstelling E: Ja, en dat is goedgekeurd door het bestuur. Onderdeel daarvan is dat de mensen van de bestuursstaf waarmee ik gesproken heb die zijn nu lid geworden van het zogenaamde p-team, het privacyteam. En zij zijn degene die de afhandeling doen van de meldingen die er komen maar ook die zich bezighouden met allerhande zaken die te maken hebben met privacy. Dus op het moment dat je, we zijn bijvoorbeeld nu bezig met het kijken naar een nieuw labsysteem, dat betekent dat er bloed geprikt gaat worden, dat betekent dus persoonsgegevens, bijzondere persoonsgegevens, dus dan moet je uitzoeken ja hoe zit dat dan met de verantwoordelijkheid, wie is de bewerker, verwerker, een hele trits zaken en dat bespreken we met het p-team om te kijken in hoeverre er rondom dat onderwerp maatregelen nodig zijn.

RS: Oke dus daar denkt het bestuur ook over mee. En de meldingen die worden afgehandeld bij het bestuur zei je?

Zorginstelling E: Nou de bestuursstaf. Het bestuur zelf zal niks doen met de meldingen. Wat we hebben gedaan. We hebben een protocol opgesteld, een protocol Meldplicht Datalekken en dat hebben we gecommuniceerd aan de hele organisatie, dat brengen we met regelmaat onder de aandacht. En daarin staat eigenlijk van nou wat moet je doen als je een issue hebt waarvan je denkt 'goh daar zouden wel eens persoonsgegevens bij betrokken kunnen zijn'. Bijvoorbeeld ik mail een cliënt om die uit te nodigen om te komen praten en je komt erachter dat je de mail naar de verkeerde persoon hebt gestuurd, oeps. Nou dan moet je dus gaan melden, en dan bedoelen we melding intern he, dus bij het p-team. En dan gaat het p-team die gaat aan de slag met die mensen en met mij ook van 'goh is er sprake van een datalek of niet?' Nou dat gaan we dan uitzoeken en daar betrekken we eventueel ook de lijn bij en het bestuur komt daar niet bij kijken.

RS: Nee en als er dan bijvoorbeeld wel sprake is van een datalek gaat het dan wel in overleg met het bestuur of iets gemeld wordt?

Zorginstelling E: Nee, niet perse laat ik het zo zeggen. We hebben nu iets van vijf meldingen gedaan bij de Autoriteit. Zoals wij het zien, zijn het steeds leermomenten 'never waste a good crisis'. Dus we gebruiken het om alerter te worden en om te ontdekken waar bijvoorbeeld zwakke plekken zitten in bijvoorbeeld onze infrastructuur en dat kan leiden tot een advies van 'joh we moeten het anders gaan doen'. Een voorbeeld daarvan is dat we nu 17 meldingen hebben gehad op het gebied van cliëntendossiers die bij printers liggen, dus bij printers in de gang en we hebben natuurlijk getoetst van hoe kan dat nou dat dat gebeurt want we hebben toch de mogelijkheid om beveiligd te printen, dus dat mensen naar hun mailbox printen en dan moeten mensen naar de printer lopen en daar hun mailbox openen en dan kiezen van stuur het er nu maar uit. Maar ze kunnen kiezen om dat niet te doen, ze kunnen kiezen om dat niet standaard te maken en dat gebeurt en dan is het de vraag van 'goh hoe breng je dat nu onder de aandacht van 1800 medewerkers?' En die 1800 medewerkers die worden allemaal op de nek gezeten om patiëntgebonden tijd te besteden, het is echt een beetje een soort van crisistijd in de zorg, dus ik kan niet met een pak papier aankomen en zeggen hier heb ik helemaal beschreven wat je allemaal moet doen, hier heb je dat lees dat maar eens. Daar hebben de mensen geen tijd voor.

RS: Nee, want hoe hebben jullie dat met dat protocol bijvoorbeeld gedaan, hoe hebben jullie dat onder de aandacht gebracht?

Zorginstelling E: Nou we hebben twee manieren waarop je standaard kunt communiceren met medewerkers en dat is het intranet en daar hebben we een berichtje op gezet. Als mensen inloggen dan starten ze meteen op met de nieuwspagina van het intranet, ze krijgen meteen dus nieuws te zien. De bevinding is wel dat dat eigenlijk nooit gelezen wordt, dat wordt meteen weggeklikt. Maar goed het is een manier om te communiceren dat is één kant en we hebben een maandelijkse uitgave van ons nieuwsblad en daar staan dan zaken in en dat wordt wel gelezen en daarin hebben we dat ook onder de aandacht gebracht. We hebben een kwaliteitssysteem waarin al onze kwaliteitsdocumenten staan en daar is dit één van dus mensen kunnen het

altijd vinden. We hebben daar ook wel vrij veel reacties op gehad, dus we hebben wel het gevoel van 'hee het is gelezen. Mensen hebben er wat meegedaan'.

RS: Want dan krijg je mailtjes van medewerkers of iets dergelijks?

Zorginstelling E: Ja, we kregen een toename van meldingen en dat is goed. En je zou denken van nee dat is niet goed, maar dat is juist goed. Zo zien we dat in ieder geval.

RS: Dan weten mensen ervan natuurlijk. En want het is natuurlijk een vrij grote instelling, hoe bereik je de verschillende groepen, want er zijn denk ik verschillende soorten medewerkers, misschien ook huishoudelijke hulp en dergelijke?

Zorginstelling E: Nou wij hebben wel een standaard infrastructuur, een standaard werkomgeving, dus dat verschilt niet van groep tot groep. Iedereen komt op dezelfde manier op het systeem en krijgt daardoor dus eigenlijk toegang tot dezelfde communicatie.

RS: En iedereen kan inloggen in dat systeem dus ook bijvoorbeeld huishoudelijke hulp?

Zorginstelling E: Nou huishoudelijke hulp zodanig als die mevrouw die hier net met de stofzuiger bezig was niet, die heeft geen werkplek als zodanig, die heeft niet de noodzaak om zich bezig te houden met de infrastructuur.

RS: Nee, maar zeg maar de medewerkers die zorg verlenen die zijn allemaal op locatie?

Zorginstelling E: Wat bedoel je met op locatie?

RS: Nou je hebt natuurlijk bijvoorbeeld ook instellingen waar veel mensen bij de mensen thuis werken.

Zorginstelling E: O ja, maar dan hebben ze een laptop van de zaak en die laptop van de zaak, die sluist hen automatisch door naar dezelfde omgeving.

RS: Oh oké, maar ze kunnen wel altijd op een plekje hier terecht?

Zorginstelling E: Ja, dat kan ook en nogmaals als zij dus bij een cliënt op bezoek zijn dan zitten ze met hun laptop bij de cliënt en die laptop is dan verbonden met ons systeem, dus dan zien zij ook weer het intranet als zij opstarten en dan ook in hun mail krijgen ze het nieuwsblad. Maar dat is één kant van de zaak. Een ander ding waarvan we dachten het is redelijk passief hè je informeert ze en dan hoop je maar dat mensen het lezen en dan is intranet niet handig merken we. Ons nieuwsblad is handiger, maar het is nog steeds passief want we hebben nu een paar maanden terug hebben we dat in ons nieuwsblad gezet, maar nu staat het niet in ons nieuwsblad en nu leest men dat niet, dus hoe blijft dat leven? Dus wat we gedacht hebben en dat is naar voorbeeld van een andere zorginstelling. Ik heb met de functionaris gegevensbescherming daar gepraat en we hebben hun idee overgenomen. We hebben stellingen ontwikkeld, simpele stellingen. Even denken nou ja bij wijze van spreken je wilt een uitdraai van een cliëntendossier maken wat doe je? En dan vier opties ofzo: je print het naar de printer, of je print het via beveiligde mailbox of je stuurt het naar je mail en je print het thuis. En die stellingen met antwoorden die sturen we naar alle teammanagers, zodat het meegenomen kan worden in het wekelijks of tweewekelijks of maandelijks teamoverleg: één stelling per keer per team. Dus roep maar wat denk jij en wat denk jij en wat denk jij en er is geen goed antwoord of slecht antwoord in die zin daar gaat het niet om het gaat er wel om dat mensen leren na te denken van 'hee kan ik dat nou zomaar op mijn bureau laten liggen of niet'.

RS: Oké dus dat ze erover na gaan denken, dus ze worden er dan wel een keer per week aan herinnerd. En wie zitten er dan bij zo'n teamoverleg?

Zorginstelling E: Nou de behandelteams bijvoorbeeld. Ook de mensen die de wijk ingaan die hebben elke ochtend een start en die hebben dus een teammanager en die hebben dus een plek waar ze dan overleggen en vanuit die agenda vanuit de bestuursstaf wordt dan gezegd van jongens je moet dat onderwerp op de agenda zetten en dat is nog niet uitontwikkeld. De manier waarop we het willen doen is, we zijn ook aan het werken

aan een eigen pagina van een eigen stukje op het intranet en dan is het idee dus dat je de stelling van de week krijgt en dat je die stelling bespreken ze en op het intranet staat dan voor de stelling van de week een soort toelichting en wel hierom is het handig dat je die persoonsgegevens niet openlijk laat liggen en dan volgende week is het weer een ander verhaal, maar die uitwerking die moeten we nog schrijven.

RS: Oké dus het is nog niet in gang getreden zeg maar.

Zorginstelling E: Nee, dat is onderdeel van het plan van aanpak.

RS: Nee, oké dus daar zijn jullie nog niet mee bezig, want ken je toevallig ook de campagne van de NVZ? De 'ZEKER' campagne?

Zorginstelling E: Ja ik heb toevallig…

RS: Oh je hebt het toegestuurd gekregen zie ik.

Zorginstelling E: Ja, die gaan we ophangen in november, dat is het al dus.

RS: Ja, dat soort dingen gaan altijd zo natuurlijk, maar ook die online quiz bijvoorbeeld die ze hadden?

Zorginstelling E: Ja, hebben we ook mee geadverteerd ook op het intranet en in het nieuwsblad en daar hebben van de 1800 medewerkers wel 40 aan meegedaan.

RS: Ja, want in totaal hadden er volgens mij 80 zorginstellingen aan meegedaan en in totaal hadden er dan iets van 2000 medewerkers gereageerd, dus dat is per instelling ook niet zoveel. Sommige instellingen zullen wat kleiner zijn, sommige wat groter. En wat vond je van die campagne?

Zorginstelling E: Ik vond het wel leuk, het was ludiek hè. Wat ik heel leuk vond was dat het niet het zwerende vingertje was. Mensen zien iets grappigs een beetje slepen en klikken. Je ziet zo'n buisje met water vullen van hoever je bent met je vragen en het kost niet zoveel tijd en het is toegankelijk, dus leuk als onderdeel van het totaalplan vooral heel goed denk ik. Ik blijf toch wel op de mening toegedaan dat je moet blijven herhalen. Anders dan gaat het niet leven. Het is niet iets, het is helemaal geen populair onderwerp, het is niet sexy het spreekt niet tot de verbeelding.

RS: Nou en toch is er natuurlijk in de media enorm veel aandacht voor de laatste tijd echt sinds september ongeveer lees je er elke week wel weer artikelen over, kan ook zijn dat het mij opvalt natuurlijk omdat ik er persoonlijk in geïnteresseerd ben, maar er komen ook wel collega's naar me toe van ik heb weer iets gelezen en weer iets gelezen, dus het komt wel steeds meer. En je ziet natuurlijk ook veel datalekken gebeuren, veel verschillende in veel verschillende instellingen van gemeenten tot ziekenhuizen. Ja, wat zijn voor jullie denk je de specifieke risico's of gevolgen die zo'n datalek voor een instelling zouden kunnen hebben?

Zorginstelling: Ja, nou dan heb je het alleen maar over de gevolgen voor de instelling. Ik vind het belangrijker nog dat de doelgroep van ons die is bijna per definitie zwakker zou ik maar zeggen he dus ja wij behandelen jongeren bijvoorbeeld ook en mensen met een psychische aandoening mensen met geen goed verweer, dus die moet je goed beschermen. Als de behandelgegevens, dat zijn onze kroonjuwelen als die op straat komen te liggen, dan vertrouwt een client ons niet meer en dan heeft die client mogelijk echt wel grote persoonlijke schade. Dus dat is een ding, dat is voor ons zeer zwaarwegend. Qua instelling hebben we reputatieschade. We willen niet in het nieuws komen dat er dossiers van clienten op straat komen. Ja, kijk een ander gevolg is natuurlijk op het moment dat je dan een bezoek krijgt van de AP en ze vinden dat je op een bepaald punt grof nalatig bent geweest, verwijtbaar nalatig en je krijgt een boete nou ja die zijn enorm fors en dat wordt met de Europese Privacy Verordening vele malen forser, dus dat kunnen we ook niet hebben, dat trekken we niet. Dus we moeten er echt alles aan doen om dat te voorkomen.

RS: Ja, en zijn die gevolgen dan ook in beeld bij het bestuur?

Zorginstelling E: Ja, ja.

RS: Want ik kan me voorstellen dat er nog andere thema's zijn die ook aandacht verdienen, maar het krijgt wel voldoende aandacht?

Zorginstelling E: Ja, het mooie is natuurlijk dat de boete is hoofdelijk, dus de boete waarvoor onze bestuurder eigenlijk aansprakelijk is. En het kostte twee zinnen in een mailtje: 'Jij gaat die boete betalen, wat wil je dat we gaan doen? En die boete is 820.000 euro per keer'.

RS: Ja, ligt er waarschijnlijk ook wel een beetje aan hoe hoog die boete is wat je precies hebt gedaan.

Zorginstelling E: Ja, tuurlijk. Ik ben er wel voorzichtig mee geweest met bespreken omdat ik er zelf een hekel aan heb en dat zie je nu veel gebeuren dat die datalekken daar springen heel veel leveranciers op dat onderwerp en die hebben zoiets van wij hebben een product en daarmee raak jij in control en als ze dat nou zouden zeggen dan zou ik het nog oké vinden maar wat ze zeggen is: 'Weet jij wel dat jij 820.000 euro boete kunt krijgen? En dat is vreselijk, je gaat failliet'. En dat is een soort insteek op basis van angst waarvan ik denk 'ja dahaag, we moeten het goed regelen'.

RS: Ja, want je krijgt natuurlijk een boel verzoeken van dat soort instellingen. Ik kom er ook een boel tegen op internet. En in hoeverre denk je dan dat communicatie een rol zou kunnen spelen in het inperken van de risico's?

Zorginstelling E: Nou kijk, ik vind je hebt een aantal plichten als organisatie om je aan te houden: dat je je gegevens goed beveiligd en dat je maatregelen neemt technisch en organisatorisch om ervoor te zorgen dat er geen datalek ontstaat, maar wat wel gebeurt. Ja, dat kan gebeuren en dan moet je je best doen om dat te voorkomen of om schade in te perken en je moet de mensen erover inlichten en je moet er als organisatie van leren en je moet het de volgende keer beter doen. Onze portemonnee is niet groot genoeg om alle maatregelen te nemen die je zou kunnen nemen om dat beveiligingsniveau omhoog te brengen, dus de communicatie is heel belangrijk in hoe je hiermee omgaat als organisatie vind ik. De manier waarop we dat doen is dus door veel de hort op te gaan door veel het onderwerp te bespreken, bewustwording proberen te kweken door bijvoorbeeld die stellingen en dat onder de aandacht te brengen, mensen snel terugkoppeling te geven. Bijvoorbeeld er was een incident waarbij een medewerkster een foutmelding op haar scherm kreeg en ze drukte op printscreen en stuurde de hele printscreen naar de helpdesk en onze helpdesk is geoutsourcet dus dat is een ander bedrijf. En zij hebben wel een geheimhoudingsplicht ondertekend, maar op het scherm stonden ook nog patiëntgegevens open. Het elektronisch patiëntendossier stond daarachter en dan denk ik ja dat hebben ze niet nodig om te weten dat zijn persoonsgegevens daar moet je alert op zijn. Dus we hebben meteen contact gezocht met degene die dat meldde en gezegd van wat goed dat je het meldt want dat is het denk ik ook je moet mensen wel een soort van belonen dat ze hun best doen. Toen hebben wij ook contact opgenomen met de helpdesk van 'joh wees je ervan bewust dat als jij een melding krijgt: eigenlijk moet jij zeggen ik wil helemaal niks weten van patiëntgegevens of persoonsgegevens want dat heb ik helemaal niet nodig voor de uitvoering van mijn werk. Nee, ik moet een storing kunnen analyseren dus ik wil een foutboodschap ofzo maar verder niet'. Dus ook aan hun kant heb ik dat goed uit zitten leggen van 'joh wees je daarvan bewust'. Ik weet bijvoorbeeld dat de leverancier van ons EPD hun helpdesk is daar heel expliciet in die zijn daar goed in getraind. Die geven ook echt aan aan melders van 'joh deze informatie hoeven we niet te hebben, die willen we niet hebben dat moet je bij je houden'. En dan ben je denk ik goed bezig. En dat stuk communicatie, je moet het onder de aandacht blijven brengen. Ik blijf herhalen.

RS: Ja, want zie je nu ook veranderingen sinds de meldplicht is ingevoerd dat mensen er meer mee bezig zijn in de organisatie?

Zorginstelling E: Nou ik heb niet echt nog gegevens om dat te vergelijken. Ik zie natuurlijk wel het feit dat er gemeld wordt. Er wordt gemeld met een redelijke hoeveelheid maar ik denk dat dat meer zou mogen zijn en voorheen ja kijk de geheimhoudingsplicht, de medische geheimhoudingsplicht zit bij veel mensen goed tussen de oren dus er zit al een groot gevoel van awareness van clientgegevens mag je niet zomaar delen. Ik kan nog niet echt zien dat de bewustwording hoger is geworden ofzo.

RS: Nee, en die protocollen waarover je vertelde waar kunnen mensen die vinden via dat systeem?

Zorginstelling E: Ja, ze kunnen via intranet zoeken, ze kunnen het nieuwsbladbericht erbij pakken als ze die nog weten te vinden, ze kunnen via het kwaliteitssysteem en daar wordt iedereen in getraind, iedere nieuwe medewerker krijgt een training dan kunnen ze het via het kwaliteitssysteem opzoeken. En op het moment dat zeg maar die intranetpagina er is, dan staan daar ook allerhande makkelijke links zodat ze dat ook makkelijk weten te vinden.

RS: Ja, want hoe is dat protocol dan ingericht? Staat daar op mail naar die persoon of?

Zorginstelling E: Ja, wil je het zien?

RS: Ja, kan wel eventjes.

Zorginstelling E: Als het goed is had ik hem namelijk al klaar gezet. Ik dacht jij gaat dat soort dingen wel willen zien. Dit is het protocol en dit is ons kwaliteitssysteem en dan een stukje inleiding, wat is een datalek, wat voorbeelden een soort beslisboom van: wanneer moet er nou daadwerkelijk gemeld worden aan de autoriteit. Wie gaat hierover? Wie speelt hier een rol over? Dat is het p-team die bovenste ben ik. Nou wat moet je doen: Meld het direct via dit e-mailadres, informeer je leidinggevenden doe een veiligheidsmelding, dat is het VIM.

RS: Ja, ik ben bekend met de VIM.

Zorginstelling E: En dan gaat het privacyteam aan de slag en nog meer en nog meer en ook met de lijnorganisatie als er nog vragen zijn natuurlijk.

RS: En het privacyteam gaat dan aan de slag en wordt er ook teruggekoppeld dan naar de medewerker?

Zorginstelling E: Ja, zeker. Dat is erg afhankelijk ook wel van de aard van de melding. Sommige dingen zijn toch wel heel erg stom. Er is een locatie zeg maar waar de medewerkers het niet tussen de oren krijgen dat ze naar beveiligde docs moeten printen en daar krijgen we vaak meldingen van cliëntgegevens die op de printer liggen.

RS: Ja, maar hoe komt dat dan dat ze het wel gaan melden?

Zorginstelling E: Zij melden het niet. Iemand, een kwaliteitsadviseur die verbonden is aan dat centrum. Die doet tegenwoordig zo'n ronde om te kijken van vis ik daar nou nog wat op? En ja hoor: en dan maakt hij een melding en dan hangen wij aan de telefoon met degene die dat geprint heeft om te zeggen van ja dat moet je niet doen. En dat werkt niet, dus we doen het ook aan zijn leidinggevende dat zeggen we ook en de teammanager en we hebben het inmiddels ook doorgesluisd naar de algemeen directeur van dat centrum. En het staat nu ook in de jaarrapportage in de kwartaalrapportage van mij aan het bestuur van nou dit is een issue. Een niet uit zichzelf te corrigeren issue zeg maar. Dus mijn advies daarop is om te starten met een proefconcept voor follow-me printen. En het idee daarachter is van mensen hebben maar één printer en kunnen niet meer kiezen.

RS: ja, dat hebben we op de universiteit ook inderdaad.

Zorginstelling E: Relatief simpel te implementeren vonden wij.

RS: Ja, maar dan blijf je natuurlijk het probleem houden dat mensen het naar hun thuismailadres kunnen sturen om het daar te printen.

Zorginstelling E: ja, maar oké. Maar als je gaat analyseren welke lekken er allemaal zouden kunnen gebeuren, dat krijg je nooit allemaal gedicht. Dus ik vind het logisch dat mensen proberen te printen en dat is voor hun werk is dat verklaarbaar en dan moet je dat faciliteren op een zo veilig mogelijke manier. En op het moment dat we dat hebben gedaan dan hebben we dus meer dan vijftig procent van onze datalekmeldingen die hebben we dan afgedekt.

RS: Ja, omdat daar dus heel veel binnenkomen.

Zorginstelling E: En als dan blijkt dat mensen persoonsgegevens meenemen naar huis. Ik kijk niet in mailboxen dat kan ik niet en dat mag ik niet. We hebben daar wel gedragsregels over afgesproken met elkaar maar ja als daar een incident uit voortkomt dan gaan we daar wel weer op acteren.

RS: Ja, want de medewerkers die nu dan die mail of die printer verkeerd gebruiken krijgen die daar gesprekken over of?

Zorginstelling E: Nou ja er zitten nog geen consequenties aan verbonden voor het personeel. Er zijn een aantal dingen te bedenken waar dan wel consequenties aan te verbonden zijn. Kijk de printer in kwestie staat in een afgesloten ruimte die alleen maar toegankelijk is voor personeel, maar huishoudelijk personeel komt er niet bijvoorbeeld en cliënten al helemaal niet. Dus dat is dan geen grond om te zeggen van het komt in je beoordelingsgesprek terug.

RS: Ja, het is dan ook, tenminste ik zou dan ook snel het idee hebben van we zitten hier toch in een beveiligde omgeving waarom mag dat niet. En bijvoorbeeld als je kijkt naar het EPD-systeem waar je toegang toe kan krijgen. Heb je daar controle over kan je zien wie waar wanneer in geweest is?

Zorginstelling E: Ja, dat is in te zien. Ik niet, ik kan dat niet zien, dat wil ik ook niet. Er is een soort procedure voor dat de zorgadministratie met een leidinggevende daar wel eens met zijn tweeën naar kijken. Daar moet dan een grond voor zijn.

RS: Ja, maar daar bemoei jij je verder niet mee?

Zorginstelling E: Nee, ik bemoei me daarmee in de zin van: ik moet weten dat dat kan ik wil weten dat dat netjes gebeurt dus als ik dat weet dan ben ik blij. Ik weet dat bijvoorbeeld in een van de afhandelingen van zo'n melding is het noodzakelijk gebleken om daar naar te gaan kijken zo van 'goh heeft die persoon dan toegang gehad tot het cliëntendossier of wat hoe zat dat'?

RS: Ja, oké en jullie hebben nu een aantal meldingen ook bij de Autoriteit Persoonsgegevens gedaan. Hoe kijk je tegen die rol aan van de autoriteit?

Zorginstelling E: Uhm, nou de autoriteit is voor mij op dit moment nog wel een beetje een onduidelijke entiteit als zodanig en ik weet wat hun bevoegdheden en hun rol is maar ik heb niet met ze te maken gehad nog. Ik ben wel geregistreerd bij hen als zijnde FG. Dus wij hoeven bij hen geen meldingen te doen over onze bewerkingen dat kan ik zelf dan bijhouden en dat hou ik ook bij. Ik ga ze binnenkort benaderen met een vraagstuk. Ik verwacht dat ik hen daarvoor mag benaderen en ja ik weet het niet. Het is een onbekende eenheid, een grootheid, ik heb nooit met ze te maken.

RS: Nee, je hebt geen contact met ze gehad ofzo?

Zorginstelling E: Nee, nee ook geen reden toegezien zeg maar.

RS: Nee, en nog iets teruggezien van de meldingen?

Zorginstelling E: Nee, nee. En kijk in het begin was het heel lastig hè waren ze helemaal understaffed. Dus toen kregen we bijvoorbeeld geen registratie terug van meldingen. En dan moest je bellen van ik heb net een melding gedaan maar ik weet de code niet en dan krijg je een student aan de telefoon en ja die wist het ook niet dus dat is niet handig. En later is dat meer op orde gekomen. Ik verwacht ook niet dat zij daarover terugkomen. In ieder geval niet gezien de aard van de meldingen die wij gedaan hebben dat is allemaal zo kleinschalig eigenlijk daar wijst niet uit dat er een grove nalatigheid is aan onze kant ofzo. Dat is niet om ons op de borst te slaan, maar we hebben gewoon denk ik de bescherming wel aardig op orde, dus gelukkig hebben we nog niet gek veel ernstige dingen meegemaakt.

RS: Nee, en toen de Meldplicht Datalekken er kwam hebben jullie toen informatie van de autoriteit ontvangen of iets dergelijks?

Zorginstelling E: Uhm, even denken nou ik weet dat er informatie beschikbaar was via de website van de autoriteit, maar hier heb ik zeg maar vanaf het moment dat het onderwerp bij mij op de radar kwam heb ik dat in de gaten gehouden en ben ik gaan lezen en uit zitten pluizen. Ik geloof dat er een brief is geweest van de autoriteit aan alle GGZ-instellingen, maar die is verstuurd naar de bestuurder, die heb ik niet gekregen, omdat ik ook toen nog geen FG was volgens mij.

RS: Volgens mij is die brief sowieso gericht naar bestuurders ook geweest. Ik denk dat dat ook wel belangrijk is, want zoals je al zei zij zijn hoofdelijk aansprakelijk. En je had het over dat plan van aanpak voor de komende twee jaar is dat voor de Europese Verordening om daarop voorbereid te zijn?

Zorginstelling E: Dat houdt er rekening mee ja en dat is best een klus. Mijn redenering was eigenlijk van ja we doen een hoop dingen al goed maar ook een hele hoop dingen echt niet. En als ik nu kijk naar hoe iedereen nu knel zit in zijn tijd en knel zit in zijn budget ja hoe sterk pak je uit met je maatregelen? Dus ik had eigenlijk het idee van nou we moeten stapsgewijs, gefaseerd toewerken naar het verhogen van je bescherming en dat betekent ook sec genomen zijn er een aantal verplichtingen waar we op dit moment echt niet aan voldoen en zeker als straks die Europese Verordening tot kracht wordt, als die straks gehandhaafd gaat worden dan hebben we een uitdaging omdat je dan met je accountability zit. Bijvoorbeeld Data interoperabiliteit ook zo'n mooie maatregel. Maar accountability dat betekent: je moet kunnen laten zien dat je doet wat je doet en wat je doet en niet alleen maar zeggen van ik heb een informatiebeveiligingsbeleid maar je moet echt zeggen ik heb dit gedaan en je moet de werking ervan kunnen aantonen maar ook op 26 februari 2017 moet je ook kunnen laten zien van toen werkte het ook en als je nu kijkt naar de verschillende gegevensverwerkingen die we kennen heb ik er 38 kunnen identificeren. Voor veel daarvan geldt dat we geen dergelijke accountability hebben dat hebben we niet in place. Dat kost tijd om dat goed op te tuigen en dat kost ook geld. Sommige systemen die zijn bijvoorbeeld gebouwd door een paar enthousiastelingen, door hele professionele enthousiastelingen maar daar is accountability niet aan de orde geweest, dus hoe ga je dat inrichten dan? Dus daarom trapsgewijs moeten wij steeds volwassener worden.

RS: En hebben jullie hier trouwens een communicatieafdeling? En wordt die ook meegenomen in het plan van aanpak?

Zorginstelling E: Ja, ik heb hier het plan van aanpak. Inleiding, meldplicht datalekken, het juridisch kader, het doel van het plan van aanpak, de samenwerking met een p-team, nou een collega is onderdeel van het p-team die draagt zorg voor communicatie. Nou in fase 1, dus ik heb het even opgedeeld in vier fasen. Eerst inventariseren en alles in kaart brengen en dan maatregelen verzinnen om compliant te zijn. In de eerste fase hebben we hier voor communicatie: dat er een protocol wordt opgesteld, dat die wordt gedeeld via het kwaliteitssysteem en in het nieuwsblad in samenwerking met de afdeling communicatie wordt een communicatieplan opgesteld en dat gaan we dan in uitvoering brengen: regelmatig terugkerende korte presentaties in teamoverleggen, privacy standaard op de agenda, maken en verspreiden van flyers zoiets als dat (wijst naar 'ZEKER' campagnemateriaal) en regelmatige berichtgeving op intranet. Dus met de afdeling communicatie hebben we nu iets van drie keer gezeten om een soort van communicatieplan op te stellen. Dat hebben ze ook gemaakt en we hebben dus ook gedacht van ik was met wat directeuren aan het praten en we hebben een beetje ons hoofd zitten breken van nou hoe bereik je nou mensen? Zeg maar behandelaren die lezen het intranet niet die hebben daar geen tijd voor, het nieuwsblad wel. Maar we hebben van die prachtige koffieautomaten met een digitaal display en als je die even niet gebruikt dan gaat hij op screensaver en dan krijg je een mooi plaatje van koffiebonen enzo. Ik had zoiets van maak dat plaatje nou een plaatje van privacy, dat mensen dus bij wijze van spreken een leuk plaatje met een cartoonpoppetje met wees geen datalek ofzo. Iedereen gaat koffie halen en dan zien ze dat. Onderdeel van het communicatieplan. Daar zitten kosten aan verbonden, want dat moet gemaakt en geïmplementeerd worden. Dat moet met usb-sticks op die koffiezetapparaten gezet worden.

RS: Ja, dat kost tijd. Je hebt natuurlijk nog twee jaar. In hoeverre denk je dat jullie voorbereid gaan zijn in mei 2018?

Zorginstelling E: Nou ik denk dat we het goed op gang krijgen. We hebben de gegevensverwerkingen in kaart, we zijn de bewaartermijnen in kaart aan het brengen. Dat betekent dus ook dat je intern moet afspreken over van wanneer ga je dingen vernietigen want je mag het niet langer bewaren dan strikt noodzakelijk. Ik denk dat we op 80% zitten, laat ik het zo zeggen. Want die overige 20% dat zit hem vrees ik in bestaande systemen zoals ons EPD. Data interoperabiliteit is ook zo'n ding uit de Europese Privacy Verordening en ja dat is een complex verhaal. Je bent verplicht om mensen in een elektronisch leesbaar formaat gegevens mee te geven als ze vertrekken naar een andere partij. Nou de letter genomen kun je dan gewoon een dump maken van je hele database in XML-formaat en dat geven en succes. Maar dat werkt niet mensen hebben daar niks aan. Mensen kunnen daarmee niet naar een andere GGZ gaan en zeggen van hier heb je mijn dossier. Het is technisch leesbaar maar het is betekenisloos. Dus je moet zien te komen op dat niveau tot een soort marktstandaard van gegevensuitwisseling.

RS: En dat zit niet in het EPD verwerkt?

Zorginstelling E: Dat zit niet in het EPD verwerkt en dat is ook lastig want we hebben een EPD van organisatie A, maar als iemand verhuisd dan komen ze bij een GGZ die gebruik maakt van een EPD van organisatie B. En dat is een andere opzet. Dus de informatie in het systeem van organisatie A is misschien niet leesbaar voor organisatie B.

RS: Ja, oké.

Zorginstelling E: En is het nu onze plicht om te zorgen dat organisatie A en organisatie B met elkaar om tafel gaan zitten? Is dat de geest van de wet? Is dat de letter van de wet? Op dat punt zijn we in ieder geval absoluut nog niet klaar.

RS: Nee, maar ik denk dat niemand daar dan nog echt klaar voor is.

Zorginstelling E: Nou weet je wat het is voor nieuwe systemen zal gaan gelden dat we dat dus gaan uitvragen. Dus als er een nieuw salarisverwerkingssysteem ofzo komt als dat soort systemen nu aangeschaft moeten gaan worden dan zeggen we tegen zo'n leverancier laat maar zien dat jij dat kan, accountability. En dan is dus het advies in de richting van de Raad van Bestuur als ze dat niet kunnen aantonen dan mag je er niet mee in zee gaan, want EPV. En dan kan dus nog steeds de Raad van Bestuur besluiten van ja gezien de huidige stand der techniek, zien wij geen alternatief in de markt om zo'n salarisverwerkingssysteem aan te schaffen. Nou dan vind ik dan zijn we weer 100%. Dan kan je zeggen van ja leuk dat je dat zegt, de elektronische uitwisseling, maar daar is de markt niet klaar voor en dat is niet ons pakkie aan zeg maar.

RS: Nee, precies.

Zorginstelling E: Dus ik denk ja, dat we 80% klaar zijn.

RS: Op dit moment of dan?

Zorginstelling E: Nee, dan. Op dit moment moeten we echt nog veel verder de plaatjes inkleuren van de verwerkingen die we hebben. Ik vind dat we voor awareness dat vind ik echt een speerpunt van mijn plan van aanpak dat moet vele malen hoger zijn dan dat het nu is het moet een soort in de genen komen te zitten dus ja we moeten voorlopig nog wel even de komende anderhalf jaar blijven communiceren dus daar hebben we dat plan voor.

RS: Ja, en hebben jullie dan ook een manier om te evalueren?

Zorginstelling E: Ja, nou wat we nu aan het doen zijn is het inventariseren en het verzinnen van zinvolle stappen en dan in fase 2 gaan we dat expliciet uitvoeren en uitrollen en daar zijn we natuurlijk al mee bezig maar daar is fase 2 eigenlijk echt voor. In fase 3 dat heet reflectie en borgen dus dan gaan we het evalueren. Dus dan gaan we kijken van hoe is dat nu gedaan, moeten we het aanpassen of bijstellen?

RS: Ja, en op dit moment is er nu een beeld van hoe het bijvoorbeeld met de awareness is in de GGZ-instelling of met bijvoorbeeld beveiligingsmaatregelen?

Zorginstelling E: Ja, dat laatste wel. Awareness is lastig te kwantificeren. Je kunt er wel een indicator voor verzinnen in de zin van hoe vaak wordt er nu een melding gedaan, dat kun je meten. En voor de beveiligingsmaatregelen daar zie je toch, want ik ben een privacyhuishouding aan het voeren dus ik registreer al dat soort zaken. En wat we dus ook doen is als je alle maatregelen wilt nemen die je kunt nemen om compliant te worden dan heb je een portemonnee nodig dus ik vind dat niet reëel dus daarom doen we dan ook een risicoanalyse op elk systeem dus dat is ook een bewijs dat we een privacy impact assessment uitvoeren en daarin zit dus van ja welke maatregelen hebben we al wat is de aard van die gegevens? Hoe spannend is dat? Wat is nou het risico dat daar een datalek in gaat ontstaan? En aan de hand daarvan hebben we een lijst met de huidige maatregelen en ook een rationele afweging van waarom je dan iets kiest of niet kiest.

RS: En want doen jullie dan een nulmeting of iets dergelijks? Want die privacy impact assessment is natuurlijk best wel uitgebreid.

Zorginstelling E: Nou dat hangt ervan af, je kunt het zo uitgebreid en zo breed maken als je het zelf wilt.

RS: Maar er zijn natuurlijk wel veel punten waar je op moet letten.

Zorginstelling E: Nogmaals dat hangt ervan af hoe je het insteekt. We hebben nu nog niet echt een standaard PIA. Er is een PIA van NOREA. Dat is een bedrijf die dat heeft opgesteld en die is goed bruikbaar, maar die richt zich meer op de informatiebeveiliging dan op compliancy naar de Wet Bescherming Persoonsgegevens of de EPV. Kijk ik heb zelf zoiets van we moeten een privacyhuishouding houden en daarin zegt de wet of zegt de autoriteit persoonsgegevens van we willen een aantal dingen daarover weten en die kan ik toetsen. Bij het nieuwe labsysteem bijvoorbeeld ben ik dus eigenlijk die lijst aan het invullen van wat de Autoriteit Persoonsgegevens van een verwerking zou willen weten, dus wie is de verantwoordelijke, wie zijn de betrokkenen, welke gegevenscategorieën ken je, zijn er bijzondere persoonsgegevens wat is de grondslag wat is het doel waarvoor je ze gebruikt. Dat zijn er zes en welke maatregelen heb je genomen en zijn die afdoende dat is de risicoanalyse. Dan heb je acht vragen gesteld en dan heb je eigenlijk al een basis PIA te pakken wat mij betreft en die kun je tot in detail uitwerken, maar daar heb je meestal geen tijd voor en ik vind dat niet noodzakelijk voor sommigen wel. Soms dan is het complex.

RS: Ja, dat is met alle dingen zo natuurlijk. Er zijn altijd complexe vraagstukken, zeker in de zorgsector. Goed, ik denk dat ik alle informatie heb. Ik zal het nog even checken. Bedankt voor je tijd.

5.6 Uitwerking interview zorginstelling F

De functie van functionaris gegevensbescherming

F is in november 2009 benoemd als security officer en houdt zich vanuit die functie bezig met informatiebeveiliging. Informatiebeveiliging heeft drie kenmerken: beschikbaarheid, betrouwbaarheid en vertrouwelijkheid. Sinds maart 2010 is F daarnaast privacy functionaris. De functie van FG is sinds 2013 ook belegd bij het College Bescherming van de Persoonsgegevens. F's hoofdtaak is security officer en de andere twee rollen doet F ernaast. F is verantwoordelijk voor al het beleid omtrent informatiebeveiliging. Daarnaast doet F bewustwordingscampagnes, geeft F voorlichting en adviseert F gevraagd en ongevraagd. Daarbij beweegt F zich door de hele organisatie, dus vanaf de werkvloer tot aan de Raad van Bestuur.

Bewustwordingscampagnes

F is verantwoordelijk voor de bewustwordingscampagnes, maar betrekt er wel andere mensen bij van bijvoorbeeld de communicatieafdeling. In 2011 is bijvoorbeeld een campagne gelanceerd waarbij door de hele instelling 300 gele vogeltjes zijn opgeplakt, zonder dat daar verder enige vorm van communicatie over is gedaan. Een week later zijn de vogels weer weggehaald en tot de maandag daarop is hier niks over gecommuniceerd. Mensen in de organisatie haakten op de campagne in door vogelgeluiden als achtergrondgeluid in te stellen. Het idee achter deze campagne was dat er juist reuring moest gaan ontstaan

en dat mensen zich af gingen vragen wat die vogeltjes daar deden. De week erop is een poster verspreid met een geanonimiseerde dokter daarop. Je zag deze dokter een gesprek voeren per telefoon door de galerij waar in principe andere mensen dit gesprek konden horen. Op de poster stond een balustrade met daarop het kleine gele vogeltje. Deze werd ingezet als luistervink met de centrale boodschap: we hebben hier een luistervink en voor je het weet luistert of kijkt deze mee. Deze luistervink wordt ingezet als symbool voor informatiebeveiliging.
F komt nog voldoende mensen tegen die getraind moeten worden in het herkennen van phishingmails. Een mooi voorbeeld als onderdeel van de bewustwording was een bericht op intranet over ransomware. Vlak na dit bericht heeft zorginstelling F een phishingmail uit laten gaan. Als je goed naar deze mail keek zag je dat de afzender niet de stafdienst ICT was en als je goed naar de link keek zag je dat dat ook geen zuivere koffie was. Toch hadden best veel mensen op deze mail geklikt. Zo'n bewustwordingscampagne in de vorm van zo'n mail helpt alleen al om mensen scherp te maken.
Zorginstelling F kiest een paar momenten per jaar uit voor een bewustwordingscampagne. De ene keer pakken ze het iets groter aan dan de andere keer.

Andere communicatieacties
Normaal gesproken houdt F een presentatie voor nieuwe medewerkers waarin F aangeeft wat de instelling van nieuwe medewerkers verwacht. Nu is er net een film gemaakt voor nieuwe medewerkers die de eerst volgende bijeenkomst wordt laten zien. Ook gaat F bij de afdelingen langs en doet F presentaties over informatiebeveiliging, privacy en de Meldplicht Datalekken.

Thema in beeld bij bestuur
Ideeën over dit thema komen over het algemeen bij F vandaan. Toen bijvoorbeeld de Wet Meldplicht Datalekken werd ingevoerd heeft F een document opgesteld en deze aan de Raad van Bestuur gegeven met daarbij de opmerking: 'volgens mij moeten we dit en dit gaan doen'. Soms komt het ook bij de Raad van Bestuur vandaan als zij iets signaleren of een vraag binnenkrijgen. Het is dus tweerichtingsverkeer.

Verhouding tussen privacy en de bescherming van persoonsgegevens
Er wordt geen onderscheid gemaakt tussen privacy en de bescherming van persoonsgegevens bij zorginstelling F. F vindt privacy wel een redelijk containerbegrip, waar de bescherming van persoonsgegevens veel meer duidelijkheid geeft over wat je nu eigenlijk wilt doen. Je doet eigenlijk de bescherming van persoonsgegevens om de privacy van de betrokkenen te respecteren en daar goed mee om te gaan.

Veiligheidsmaatregelen
Er worden ook veiligheidsrondes gedaan waar F ook in meeloopt. F kijkt dan of er dingen zijn op het terrein van informatiebeveiliging of privacy die verbetering behoeven. Voorbeelden hiervan zijn papierkratten of computers die open staan, terwijl deze eigenlijk netjes vergrendeld moeten worden. Dit weet ook iedereen bij zorginstelling F, daar zijn gedragsregels over afgesproken.

Onderscheid tussen verschillende groepen
Er wordt op dezelfde manier naar iedereen gecommuniceerd. F is van mening dat het niet uitmaakt wat je in de organisatie doet, voor iedereen gelden dezelfde regels. Daarom vindt F dat iedereen op dezelfde manier geïnformeerd moet worden over wat er van medewerkers verwacht wordt.

Aanspreekcultuur
In zorginstelling F heerst een aanspreekcultuur. Dat betekent dat medewerkers opletten wat er gebeurt en elkaar erop aanspreken wanneer je dingen ziet waarvan je denkt dat dit anders hoort. Niet met het idee van dat je iets fout gedaan hebt, maar meer van joh denk er even aan. Er heerst hierbij een open sfeer.

Veranderingen sinds invoering Wet Meldplicht Datalekken
Mensen zijn wel een stuk alerter geworden. Je krijgt bijvoorbeeld vragen of er een betere manier is om documenten te versturen per mail. Zorginstelling F is nu aan het kijken naar een softwarematige oplossing om mails veilig te kunnen versturen.

Communicatie-acties naar aanleiding van Wet Meldplicht Datalekken

Zorginstelling F heeft een intranet, maakt gebruik van nieuwsbrieven en van postercampagnes. Daarnaast houdt F één keer per jaar een informatiebeveiligingsmarkt waarin ook privacy aan de orde komt. Dit jaar ging dit ook specifiek over de Meldplicht Datalekken. Deze markt houdt zorginstelling F voor de ingang van het restaurant, omdat daar veel medewerkers langslopen. Ze kondigen deze markt aan op intranet en kondigen het ook weer af op intranet door de highlights hierop te presenteren. Op deze manier worden ook mensen die die dag niet aanwezig waren op de hoogte gehouden. Maar daarnaast is het echt het belangrijkste om bij afdelingen langs te gaan en daar je verhaal te vertellen. Hier houdt F dan een verhaal over informatieveiligheid. F begint meestal met social media om aan te sluiten bij de werknemer en zijn privéleven en maakt vervolgens een bruggetje naar het werk. Centraal hierbij staat wat zorginstelling F van de medewerker verwacht po het gebied van informatieveiligheid.

(Communicatie)beleid
Zorginstelling F is al zes jaar aan de slag met communiceren rondom informatiebeveiliging. Het is ieder jaar een terugkerend thema. De evaluatie van de communicatie zou nog wel wat beter kunnen. F doet wel evaluatie met mensen die betrokken zijn geweest bij een bespreking en vraagt dan wel wat de betrokkenen goed en minder goed vonden werken, maar zorginstelling F vraagt de medewerkers niet specifiek om mee te evalueren. Na presentaties vraagt F ook wel om tips.

Mogelijke gevolgen van een datalek
Het belangrijkste is dat alle patiënten erop moeten kunnen vertrouwen dat hun gegevens bij zorginstelling F in goede handen zijn, dus dat willen ze uitstralen. Dit is lastig in een ziekenhuis, omdat iedereen naar binnen kan lopen. De Raad van Bestuur wordt daarnaast ook wakker als ze weten dat ze kans hebben op een boete van 820.000 euro.

Gevolgen in beeld bij Raad van Bestuur
De Raad van Bestuur heeft de gevolgen goed in beeld. Los van die boete heb je als organisatie ook een klus die je moet uitvoeren als je met een datalek van doen hebt. Je moet ontdekken wat de oorzaak van het lek is, wat de gevolgen van het lek zijn en wat je daaraan kunt doen. Daarnaast heb je herstelwerkzaamheden als ziekenhuis om aan het basisprincipe te kunnen voldoen dat iedere patiënt op je moet kunnen vertrouwen.

Procedure Meldplicht Datalekken
Zodra je een datalek constateert is eigenlijk het eerste wat je moet doen zorgen dat F het weet. Medewerkers kunnen intern bij F melden. Dit weten zij onder andere door de presentaties van F. Daarnaast is het onderdeel van de procedure die vindbaar is op het kwaliteitsportaal. Toen zorginstelling F die procedure heeft gepubliceerd, heeft de instelling dit ook in de lijn gecommuniceerd aan lijnverantwoordelijken die dat weer door kunnen zetten naar de rest van de lijn. Op deze manier is geprobeerd dit zo breed mogelijk op het netvlies te krijgen in de organisatie. Er zijn twee methodieken om een datalek te melden je kunt F mailen of bellen of iemand meldt een incident bij de helpdesk waarbij de melder nog niet doorheeft dat het om een datalek gaat. De helpdesk heeft de instructie om bij ieder incident na te gaan of dit een potentieel datalek is en kan dan een vinkje zetten als dit zo blijkt te zijn. Dan krijgt F dit via het systeem door. F is 24 uur per dag beschikbaar voor datalekken.

Aantal meldingen
Er komen nog nauwelijks meldingen binnen. F heeft een tweetal datalekken gemeld. F denkt dat dit een goed teken is. F denkt dat zijn instructie helder is: ‘als organisatie moet je je stinkende best doen om je medewerkers goed te informeren over wat een datalek is en hoe je dit moet constateren. Weet hier dat de drempel heel laag is en dat je bij iedere vorm van twijfel meteen moet bellen’. Het kan natuurlijk zijn dat medewerkers niet melden, maar F communiceert duidelijk dat F liever heeft dat een melding intern doorkomt dan dat een betrokkene, een patiënt of medewerker gaat melden bij de Autoriteit Persoonsgegevens.

Rol van de Autoriteit Persoonsgegevens
Het is goed dat ze er zijn, maar ze hebben te weinig mankracht en dat is wel echt een probleem. Er is nog geen boete uitgedeeld, terwijl dit wel noodzakelijk is als je als organisatie slagvaardig wilt kunnen optreden. De angst moet er wat F betreft meteen af: we moeten transparanter omgaan met dit soort incidenten om een hoger kwaliteitsniveau van de bescherming van persoonsgegevens te bereiken. Uiteindelijk moeten organisaties

snappen dat de inzet is om zo goed mogelijk om te gaan met persoonsgegevens. Daarom verwijst F ook graag terug naar het basisuitgangspunt dat mensen erop moeten kunnen vertrouwen dat er goed omgegaan wordt met de gegevens van patiënten.
F geeft aan dat de AP een brief gestuurd heeft naar de Raden van Besturen van alle zorginstellingen, maar dat deze ging over autorisaties binnen het elektronisch patiëntendossier, verder horen ze van de Autoriteit niet zoveel. F heeft ze wel eens gebeld met een vraag. Die vraag is door de autoriteit nog niet beantwoord.

Voorbereiding op de AVG
Zorginstelling F is hier nog niet op voorbereid, maar is wel bezig zich hierop voor te bereiden. Voor deze organisatie heeft F in kaart gebracht wat de verschillen zijn tussen de WBP en de AVG en wat dit van de organisatie vraagt om de komende tijd op te pakken en uit te voeren. Daarbij moet je wel in je hoofd houden dat de AVG eigenlijk al is ingegaan, maar dat er pas vanaf mei 2018 op gehandhaafd wordt. Als je het heel netjes doet dan zou je dus op een zo kort mogelijke termijn ook compliant moeten zijn op de AVG. Nu is het niet zo dat er in de AVG heel veel nieuws staat .Als je je beleid als organisatie goed uitvoert dan zou je eigenlijk al voor 80% compliant kunnen zijn aan de AVG. Het gaat om die laatste 20%. Het is dan ook meer aanscherpen van wat we eigenlijk al aan het doen waren.
F heeft een actielijst opgesteld met wat er in de komende tijd uitgevoerd moet worden. De Privacy Impact Assessments gericht uitvoeren is bijvoorbeeld nog een stap die zorginstelling F nog goed in zijn proces moet inpakken.

Bekendheid 'ZEKER' campagne NVZ
F is bekend met de 'ZEKER' campagne van de NVZ, omdat die komt uit het netwerk informatiebeveiliging waar F ook lid van is. F doet zelf altijd in de weken van Alert Online de informatieveiligheidsmarkt en dan zie je ook de campagne 'ZEKER' voorbij komen. Hij haakt hier dan op in. Eén van de onderdelen van de informatieveiligheidsmarkt was bijvoorbeeld het invullen van de zekertest. Deze test kon je ter plekke invullen met een groot scherm zodat mensen konden meekijken.

5.7 Uitwerking interview zorginstelling G

RS: Dus eerst benieuwd hoe ben je op deze functie terechtgekomen het is natuurlijk vrij nieuw de functie van Privacy Officer, functionaris van de gegevensbescherming.

Zorginstelling G: Ik ben niet in dienst van deze zorginstelling, maar ik word ingehuurd. Juist ook voor dit specifieke onderwerp. Dus ja van ons uit heeft het zeker de aandacht en deze zorginstelling heeft het ook de aandacht gegeven die het nodig heeft en gevraagd of ik daar wat werkzaamheden voor wil verrichten als functionaris gegevensbescherming.

RS: Ja, want hoe ben je hier dan aan verbonden?

Zorginstelling G: Ik werk voor mezelf en vanuit die hoedanigheid ben ik hier terechtgekomen voor wat andere projecten nog en wat architectuurvraagstukken. Architectuurvraagstukken liggen redelijk dicht tegen het privacygedeelte aan zeg maar en is in principe ook een onderdeel van de NEN 7510 architectuur. Dus in die hoedanigheid ben ik begonnen zeg maar en met de nieuwe wetgeving en dergelijke is dat verder uitgebreid naar functionaris.

RS: Ja, werk je voor meer zorginstellingen dan?

Zorginstelling G: Ja.

RS: Dus hoeveel uur per week ongeveer zit je hier?

Zorginstelling G: Ja, ik zit hier een dag of drie per week gemiddeld.

RS: Oké, toch aardig wat eigenlijk. En je hebt natuurlijk privacy en je hebt de bescherming van persoonsgegevens hoe staan die twee tot elkaar in verhouding volgens jou?

Zorginstelling G: Ja, dat ligt heel dicht tegen elkaar aan wat mij betreft. Het één kan niet zonder het ander. Kijk de wetgeving is natuurlijk één, maar uiteindelijk is die ook weer gebaseerd op de NEN of de ISO-normen zeg maar en echt op privacy gericht.

RS: En werk je dan voor die andere organisaties ook als functionaris gegevensbescherming of ook wel eens in een andere functie?

Zorginstelling G: We zijn daar nu wel NEN 7510 aan het implementeren. Functionaris moet nog benoemd worden. We zijn net begonnen. Het zou maar zo kunnen dat ik dat ook word. Het zou ook kunnen dat ze intern iemand nemen.

RS: Want hier bij deze instelling ben je dan de enige hier die iets met privacy van doen heeft?

Zorginstelling G: Nou ja goed zo voelt het soms, maar dat is zeker niet de bedoeling. Informatiebeveiliging doe je niet alleen dat doe je als hele organisatie, maar het liefst stoppen ze het wel bij je weg en willen ze er het liefst zo min mogelijk mee te maken hebben. Maar goed als je het wilt borgen binnen de hele organisatie dan moet ook de hele organisatie ermee bekend zijn en je managementsysteem moet draaien, dat is het belangrijkste.

RS: En hoe ben je hier dan terechtgekomen, je deed hier al andere werkzaamheden?

Zorginstelling G: Ja, ik deed hier al andere werkzaamheden en ben dit erbij gaan doen zeg maar.

RS: Oké en kwam die vraag dan vanuit het bestuur of…?

Zorginstelling G: We hebben, ja deels vanuit het bestuur, maar we hebben ook een risicoanalyse gedaan halverwege vorig jaar en daar kwamen deze punten naar boven zeg maar dus er is wel gevraagd vanuit de directie en vanuit het bestuur om dat op te pakken zeg maar. Niet zozeer om de certificering te gaan halen, maar wel om volgens die weg te gaan werken. En ook om te zorgen dat de transformatie die ze nu doormaken om alles uit te besteden dat leveranciers wel gelijk aan de dingen voldoen waar ze aan moeten voldoen volgens ons.

RS: Ja, want als er zeg maar beleid moet worden opgesteld soms, ben jij dan degene die daar dingen voor schrijft?

Zorginstelling G: Negen van de tien keer schrijf ik het en als een ander het schrijft dan kijk ik of dat het past in het totaalplaatje, ja.

RS: En overleg je daar dan voor met de Raad van Bestuur?

Zorginstelling G: Ja, ik overleg altijd en ik adviseer altijd als ik het zelf geschreven heb om dat te accorderen zeg maar en als een ander dat geschreven heeft wat ik ervan vind en ook om het te accorderen. Ja, de Raad van Bestuur is daar altijd bij betrokken, die is ook hoofdelijk aansprakelijk.

RS: Ja, maar hoe is deze functie dan belegd in deze organisatie? Sta je direct onder de Raad van Bestuur of valt dit onder een afdeling?

Zorginstelling G: Het zit bij een afdeling ja. Denk niet dat het daar hoort. ICT is onder andere één van zijn speerpunten zeg maar. Deze instelling is verdeeld in klantgroepen en een centraal deel, dus dit valt onder het centrale deel. Maar goed als je het goed bekijkt zou je rechtstreeks onder bestuurders en staffunctie moeten zitten denk ik. Nu heeft iemand er belang mee, maar in principe is dat niet de bedoeling.

RS: Maar je hebt dan wel een directe lijn met de Raad van Bestuur om zaken te overleggen. En is hier een communicatieafdeling en ben je daar ook mee in gesprek?

Zorginstelling G: Ja, een stukje awareness en dat soort zaken doen we altijd gezamenlijk.

RS: En wat is daar bijvoorbeeld aan gedaan tot nu toe?

Zorginstelling G: We hebben laatst geflyerd zeg maar met een aantal speerpunten en ook materiaal rondgemaild. Nieuwsbrieven doen we en we zorgen dat het dan op alle locaties ligt op plekken waar mensen komen. Aan de wand gespijkerd ja.

RS: Ja, want deze instelling heeft meerdere locaties toch dit is niet de enige?

Zorginstelling G: Ja, dit is echt alleen een kantoor zeg maar en er zijn nog 12 grote locaties waar zorg verleend wordt en dan nog een stuk of 12-13 locaties met wijkteams. De teams die echt de wijk in gaan zeg maar voor de extramurale zorg.

RS: En worden al die groepen op dezelfde manier benaderd of wordt daar onderscheid in gemaakt?

Zorginstelling G: Daar wordt wel onderscheid in gemaakt tussen extramuraal en intramuraal ja. Dat zit anders in elkaar extramuraal loopt iedereen met Ipads of met dossiers op de fiets. Die komen echt bij de mensen thuis dus daar spelen wat andere dingen dan bij de teams die binnen zitten, wat in principe afgesloten ruimtes zijn. Ja dan werkt het iets anders.

RS: Ja want hoe bereik je dan die mensen die altijd onderweg zijn zal ik maar zeggen?

Zorginstelling G: Ja, eigenlijk op dezelfde manier. Daar wordt ook geflyerd en wordt ook gesproken. We hebben ook een awarenesstraining die verplicht is om te doen door iedereen.

RS: Dus als je nieuw bent hier dan moet je die training volgen en de huidige medewerkers hebben hem ook gedaan?

Zorginstelling G: Ja en de huidige medewerkers die moeten hem voor het eind van het jaar gedaan hebben.

RS: Ja, want wanneer is de training opgezet?

Zorginstelling G: Even kijken hoor dat is in ja, we hebben hem al een tijdje zal ik maar zeggen. Maar door de veranderingen en het kantelen van de organisatie hebben we iedere keer een excuus gehad om hem niet te gaan doen zeg maar. En nou ja er is nu wel gezegd in volgens mij september ofzo is die beschikbaar en tot het eind van het jaar hebben de mensen om hem gewoon te gaan doen.

RS: Ja en wat staat er dan bijvoorbeeld in die training? Want het is een online training begrijp ik?

Zorginstelling G: Ja, het is een online training voor awareness, voor informatiebeveiliging. Dus het zijn iets van 20 punten geloof ik waar je gevraagd wordt wat wel of niet goed is en als je antwoord hebt gegeven dan staat erachter een verklaring van waarom dat zo is met wat verdere tekst en uitleg.

RS: Oké dus een soort multiplechoicevragen met uitleg erbij?

Zorginstelling G: Ja, met uitleg erbij waarom iets goed of fout is of wat de beargumentering is in ieder geval.

RS: Hoe lang duurt zoiets ongeveer om in te vullen?

Zorginstelling G: Uh, ze zeggen twintig minuten, maar je bent wel wat langer bezig.

RS: Oké.

Zorginstelling G: Een half uur tot drie kwartier ben je wel zoet als je dat gewoon doet. Ook als je het goed hebt alsnog alles gaat doorlezen wat er dan achter staat.

RS: Ja, want ben je ook bekend met de 'ZEKER' campagne van de NVZ?

Zorginstelling G: Dat is de flyercampagne die we gedaan hebben.

RS: Ja, dus dat was die in oktober was opgezet?

Zorginstelling G: Ja, klopt. Twee weken ofzo was dat hè. Dus toen hebben we iedere keer wat gecommuniceerd en neergelegd.

RS: Ja, want hebben jullie dan ook toevallig die online test gebruikt?

Zorginstelling G: Ik heb hem zelf wel gedaan, maar we hebben hem niet gebruikt. Omdat we ook zelf al een test of een training hebben lopen, vond ik het een beetje dubbel. Dus dat hebben we niet gedaan. Maar dat is misschien voor een vervolg weer wel een goede optie.

RS: Want je hebt hem zelf wel gedaan zei je? Wat vond je van de test?

Zorginstelling G: Ik zit even te denken, ik heb hem toen gedaan, maar ik zou het zo niet meer weten wat ik ervan vond.

RS: Nee, het waren dan verschillende multiplechoicevragen inderdaad over informatiebeveiliging.

Zorginstelling G: Ja, het kwam een beetje overéén zeg maar en het is voor kantoormedewerkers wat we hebben en met mail maar ook gewoon fysiek. Mag je een foto maken van iemand om te kijken met je collega hoe je daarmee om moet gaan of zoiets. Nou dat mag van iets, maar niet herkenbaar en dat soort dingen. Whatsapp hè mag je dat gebruiken en dat soort dingen allemaal. Dus echt heel breed zeg maar opgezet en dat is op zich wel goed.

RS: Ja, want zijn hier gedragsregels opgesteld waar iedereen zich aan moet houden?

Zorginstelling G: Er zijn sowieso gedragsregels. Niet specifiek voor informatiebeveiliging op dit moment. Er is wel een soort van protocol zeg maar waarin de standaardzaken staan, maar dat is echt niet veel bijzonders zeg maar. Dat is dat je elkaar moet aanspreken op een aantal zaken, usb en dat soort dingetjes, clean desk, nou dat zijn een beetje de standaard punten.

RS: Ja, dat zijn dan een soort van methodes om te zorgen dat er geen papieren blijven liggen.

Zorginstelling G: Juist, ja.

RS: En welke gevolgen denk je dan specifiek voor deze instelling die er zijn van een beveiligingsissue, een datalek?

Zorginstelling G: Van een datalek? Ja, dat ligt eraan op welk gebied de lek is zal ik maar zeggen of het een cliëntdossier is of alle cliëntdossiers dan haal je het acht uur journaal wel zeg maar, we zijn natuurlijk een redelijk grote club. Dus ja dan heb je wel een probleem zeg maar.

RS: Op welk gebied heb je dan een probleem?

Zorginstelling G: Nou in ieder geval dat alles op straat ligt en dat je de verkeerde aandacht krijgt als organisatie zijnde. Dus op dat gebied zeker en je krijgt een boel werk. Je moet al je cliënten af je moet ze allemaal informeren en allemaal voortgang doen en ja dan wordt er nog een keer bovenop je huid gezeten om maatregelen te nemen en dan is het eigen tempo wel weg zal ik maar zeggen.

RS: En zijn deze gevolgen dan ook in beeld bij het bestuur?

Zorginstelling G: Nou ja goed zijn deze gevolgen in beeld bij het bestuur, ja dat ligt eraan of je een boete gaat krijgen of niet. Alle punten die er zijn gaan sowieso altijd via het bestuur. De bestuurders zijn altijd op de hoogte van de incidentmeldingen.

RS: Ja, dus eigenlijk want zij hebben waarschijnlijk wel meer thema's waar ze zich druk om moeten maken. Vind je dan dat het een hoge prioriteit krijgt in deze organisatie?

Zorginstelling G: Het krijgt de juiste prioriteit ja. Ze zijn er zeker van bewust dat het impact heeft.

RS: Waaraan kun je dat dan bijvoorbeeld zien?

Zorginstelling G: Er wordt snel gereageerd op mail of er wordt van hun kant uit: je wilt natuurlijk dat je alles hoort en ziet, maar dat gaat natuurlijk niet zo, dus ook vanuit die weg zijn er kanalen natuurlijk en worden er dingen besproken met andere directeuren van wat er eventueel gebeurd is en dan word ik wel meteen in de loep gezet zeg maar om te kijken hoe we dat kunnen afdekken en of er echt nog iets gemeld moet worden zeg maar.

RS: Want je hebt natuurlijk sinds 1 januari is de Wet Meldplicht Datalekken van kracht gegaan. Merk je dan ook veranderingen in je organisatie dat mensen er bijvoorbeeld meer mee bezig zijn?

Zorginstelling G: Ja, je merkt wel dat het wat meer aandacht heeft ook vanuit het management zeg maar het is iets minder vrijblijvend geworden. Het speelt natuurlijk al langer, dat je er iets mee moet en dat het aandacht nodig heeft. Maar met de nieuwe wetgeving en ook de consequenties daarvan is het wel allemaal ietsjes makkelijker geworden om acties te ondernemen zeg maar.

RS: Want hoe lang werk je hier al dan?

Zorginstelling G: Ik loop hier denk ik zo'n drie jaar.

RS: En merk je dan ook verschil dat je makkelijker beleid kan opstellen of iets dergelijks?

Zorginstelling G: Je merkt dat het nu wat makkelijker gaat. Dat is niet helemaal eerlijk misschien want we zitten midden in een omslag om alles uit te gaan besteden dus dan moet je sowieso alles op papier gaan zetten en zorgen dat het er is. Om sowieso een referentiekader te hebben en je eigen uitgangspunten helder te hebben, dus het is niet helemaal één op één dat dat door de wetgeving komt, maar dat werkt wel mee zeg maar.

RS: Want in wat voor overgangsfase zitten jullie dan? Er gaat meer uitbesteed worden?

Zorginstelling G: Ja, applicaties die buiten de deur komen te staan.

RS: Dus veel bewerkersovereenkomsten ook die daaraan vast liggen. Daar moeten dan natuurlijk regels voor opgesteld worden.

Zorginstelling G: Ja, dat is wel leuk ook om dat voor elkaar te krijgen.

RS: Wel een lastig punt ook volgens mij.

Zorginstelling G: Nee, dat is een hele lastige. Iedereen moet in principe een bewerkersovereenkomst hebben als je diensten verleend voor een ander, maar er zijn ook bedrijven waarvan ik denk ja hoezo dat wil ik helemaal niet. Ja mooi dat jij dat niet wilt maar je bent verplicht om dat te hebben en dat is niet sinds 1 januari dat is al anderhalf jaar zo. Dus het had er eigenlijk allang moeten zijn en dan nog over de inhoud zeg maar. Dus

we hebben het zelf opgesteld eentje en ja je hebt altijd discussies over wat wel kan en wat niet kan, dus het is wel altijd een dingetje zeg maar.

RS: Ja dat zal je ook altijd houden, dat is in andere werkomgevingen niet anders. En zijn er ook communicatie-acties geweest naar aanleiding van de invoering van de wet?

Zorginstelling G: Communicatie-acties naar?

RS: Communicatie-acties als in bijvoorbeeld een protocol opgesteld voor de meldplicht of communicatie door te informeren naar medewerkers dat de wet er is.

Zorginstelling G: Ja, ja zeker dat is allemaal gecommuniceerd ja.

RS: Op wat voor manieren is dat dan gegaan?

Zorginstelling G: Dat is via de directeuren gegaan zeg maar dat dat naar hun afdeling en mensen bekend is en daar hebben we, dat is onderdeel van de awareness, daar flyeren we ook voor en daar sturen we mailtjes voor, de nieuwsbrief en op de intranetpagina staan daar regelmatig stukken over van ja waar je je aan moet houden.

RS: Ja, dus dat is eigenlijk onderdeel een beetje van die awarenesscampagne die er is.

Zorginstelling G: Ja, ik zie het niet los zeg maar. We zijn dan met de NEN 7510 bezig om in ieder geval die werkwijze te hanteren en daar is dit onderdeel van. Omdat ministeries ook aangeven dat als je de NEN 7510 hanteert dat dat in principe voldoende moet zijn. Ze zijn daar voorzichtig in natuurlijk, dat snap ik ook, maar ja dat dat wel de weg is zeg maar, dus ja dan hoef je daar niet nog een keer naast nog iets te doen zeg maar.

RS: Nee en voor datalekken specifiek is daar een protocol voor opgesteld hoe medewerkers moeten melden weten ze dat?

Zorginstelling G: Ze weten waar en hoe ze moeten melden en dat is ook gepubliceerd en regelmatig gecommuniceerd.

RS: En hoe kunnen ze dan melden? Doen ze dat direct bij jou of is er een intern meldpunt?

Zorginstelling G: Ja, nou er is een intern meldpunt maar dat komt ook wel bij mij uit. Dus ja dat is er zeker. We hebben één keer in de maand ook een inloopspreekuur voor als mensen vragen hebben en daar wordt op zich ook wel gebruik van gemaakt dat mensen binnenlopen of telefonisch dat mensen echt wel komen van wij doen dat altijd op deze manier maar dat voelt niet goed.

RS: Oké, dus dat is een spreekuur één keer per maand? En dan kan iedereen in principe langskomen vanuit de hele organisatie?

Zorginstelling G: Ja, vanuit de hele organisatie ja.

RS: En doe je dat dan op verschillende locaties of doe je dat hier?

Zorginstelling G: In principe hier en dat kan ook op een locatie als dat nodig is ja.

RS: En is daar veel animo voor?

Zorginstelling G: Ja, wat is veel?

RS: Komen er mensen langs?

Zorginstelling G: Er is denk ik vier keer wel via de mail of via de telefoon gevraagd hoe moet ik dit nu zien en hoe moeten we hier nu mee omgaan?

RS: In hoeverre denk je dan dat communicatie een rol kan spelen in het inperken van de risico's?

Zorginstelling G: Nou Awareness is communicatie denk ik, dus dat is 80% van het hele gebeuren is awareness en communicatie dus ik denk dat een heel groot deel daarvan de boel kan afdekken.

RS: Je ziet het natuurlijk inderdaad: 80% van de datalekken komt door menselijke fouten. Hangt er natuurlijk ook wel van af welk onderzoek je erover leest en op wat voor manier ze het precies getest hebben. En je hebt natuurlijk nu de Meldplicht Datalekken en straks gaan we naar de Europese Verordening die is natuurlijk nu van kracht en straks wordt die ook handhaafbaar. In hoeverre denken jullie dat je daar op voorbereid gaat zijn tegen die tijd?

Zorginstelling G: Nou dat is hetgeen zeg maar waar we naartoe werken. Dan gaat het echt pijn doen vanaf dat moment als je het niet op orde hebt. Er verandert wel wat natuurlijk.

RS: Want hoe zijn jullie van plan om daarop voorbereid te zijn?

Zorginstelling G: Door te zorgen dat je op de NEN-manier werkt zeg maar dat je dat geadopteerd hebt en dat je volgens die weg werkt dat je je managementsysteem op orde hebt zeg maar. Kijk dat er nooit iets gebeurt dat kan je toch niet afdekken, dus je moet gewoon zorgen dat je managementsysteem loopt en zorgen dat je in control bent. Dan kun je ook schakelen als er iets gebeurt.

RS: En wat moet ik me dan voorstellen bij die NEN-normen? Ik heb er wel een tijdje terug iets over gelezen, maar dat is al een beetje weggezakt. Wat zijn dan voorbeelden concreet in de organisatie die moeten zijn doorgevoerd?

Zorginstelling G: Nou het zijn iets van 135-140 controls zeg maar die je als organisatie moet beantwoorden hoe je daarmee omgaat. Dus die moet je één voor één af en dan aan de hand van het business impact en de risicoanalyse kan je ze kwalificeren en dan kan je zeggen degenen die de meeste pijn doen alvast behandelen en zorgen dat je dat op orde hebt. Als je naar de NEN kijkt heb je drie jaar de tijd om alles te doen en ja dat moet je dan herhalen verbeteren en zorgen dat dat in control is. Dus dat is het idee aan de norm. Maar die is gelijk aan de ISO70001.

RS: En dat is de norm waar je toch eigenlijk nu al aan moet voldoen?

Zorginstelling G: De zorginstelling hoeft daar niet aan te voldoen.

RS: Oké dus die hebben nog de tijd om dat op orde te krijgen?

Zorginstelling G: Ziekenhuizen die zijn het wel verplicht en die hebben vijf jaar de tijd gehad en iedere keer een stapje verder. Dat is bij de VVT-markt in ieder geval nog niet zo geïntroduceerd en je bent het ook niet verplicht, maar ja hoe lang duurt het voordat het wel verplicht wordt en als het verplicht wordt dan krijgen ze niet de vijf jaar die het ziekenhuis ook heeft gehad zeg maar. Dus daarop zijn we ook al wat aan het voorsorteren en sowieso mei 2018 moet je het denk ik op orde hebben. Dat lijkt me verstandig.

RS: Ja, je hebt natuurlijk de Europese Verordening en de privacy impact assessments en dergelijke die daarbij horen en je hebt de Autoriteit Persoonsgegevens. Hoe kijk je tegen die rol aan van de Autoriteit Persoonsgegevens?

Zorginstelling G: Ja, geen idee. Ja, ik vind hem lastig. De wetgeving is er en ze zijn redelijk rustig zal ik maar zeggen, maar ik vrees wel dat ze nog voor mei 2018 een paar eruit vissen die als voorbeeld gesteld gaan worden en daar kan je beter niet bij zitten zeg maar.

RS: En heb je bijvoorbeeld van hen toen die wet inging ook informatie ontvangen of iets dergelijks?

Zorginstelling G: Nee, volgens mij helemaal niks. We hebben onszelf aangemeld als functionaris, we staan al op de site en dan krijg je een paar mailtjes van hoe het werkt en hoe je je aanmeldt. Maar voor de rest volgens mij is er niks van hun kant uitgekomen van dat het er is.

RS: Nee, en heb je zelf al eens contact met hen opgenomen?

Zorginstelling G: Ik heb ze één keer gebeld volgens mij om te kijken om iets wel of niet aan te melden. Daar kreeg ik niet echt een goed antwoord op zeg maar. Dus dat heb ik zelf bekeken aan de hand van de vragen die ze hebben als je moet melden, maar uiteindelijk hebben we twee of drie keer op het punt gestaan om iets te melden, maar uiteindelijk niet gedaan omdat je gewoon wel kon borgen dat er niks gelekt was en dat er eigenlijk niks naar buiten is gekomen.

RS: Nee, precies. Dus er zijn nog geen meldingen gedaan tot dusver bij de autoriteit? Want ben je bijvoorbeeld bekend met de NVFG, het Nederlands Vakgenootschap voor Functionarissen van de Gegevensbescherming?

Zorginstelling G: Nee.

RS: Oké nee want daar komt de Autoriteit wel eens praten, dan organiseren ze een Ronde Tafelbijeenkomst bijvoorbeeld. Ik was daarbij in september toen was Udo Oelen daar ook van de Autoriteit en allemaal functionarissen gegevensbescherming in de zaal en praten over onduidelijkheden in de wet. Maar je hebt dan geen antwoord of reactie van hen gehad?

Zorginstelling G: Nou niet iets waar ik mee verder kan.

RS: Oké en als je met zo'n probleem zit bijvoorbeeld gaat dit een datalek worden of niet ben jij dan de enige die daarover oordeelt of heb je mensen hier in de organisatie waar je bij terecht kan?

Zorginstelling G: ik kan wel bij mensen terecht ja even polsen hoe zij het zien en tot waar het gekomen is en wat er aan de hand is, maar goed ik ben daar wel altijd bij betrokken en ik doe altijd wel het advies dan of er wel of niet gemeld moet worden.

RS: En zijn er bijvoorbeeld op dit moment ook al maatregelen voor medewerkers als ze dingen niet melden?

Zorginstelling G: Nee.

RS: Als ze bijvoorbeeld hun computer open laten staan.

Zorginstelling G: Je moet elkaar daarop aanspreken. Dat zijn dingen dat kost best wat tijd zeg maar. Daarom vind ik ook dat ik dat niet alleen moet doen maar dat het ook breed gedragen moet worden. En daar zijn we nu ook mee bezig dat het vanuit het managementsysteem wat moet gaan lopen zeg maar. Een afdeling als kwaliteit mee te nemen in dit verhaal want die kijken echt naar medische stukken en naar cliëntveiligheid en dat soort zaken, maar hè dit is een kleine stap om erbij te doen denk ik dan.

RS: Ja, want zij hebben natuurlijk al kwaliteitsmeldingen en dergelijke waar zij mee van doen hebben. Ga je op zo'n afdeling dan een presentatie geven of iets dergelijks?

Zorginstelling G: Ja, dat doe ik middels presentaties, maar ook gewoon het onderdeel maken van het werkproces dat ze daar ook een actieve rol in hebben. Dus niet alleen informatief maar ook dat zij een onderdeel zijn van het geheel en zorgen dat ook daar gemeld kan worden en dat ook zij acties uit gaan zetten.

RS: Want op dit moment kan er dan alleen bij jou gemeld worden of zit dat ook in het kwaliteitssysteem verwerkt?

Zorginstelling G: Nee, dat zit nog niet in het systeem verwerkt. Daar zijn we nu wel mee bezig.

RS: En veiligheidsregels in de organisatie, zoals bijvoorbeeld het gebruik van usb-sticks?

Zorginstelling G: Daar zijn beperkte regels voor. In ieder geval dat je erop moet letten en sticks die niet van jezelf zijn niet gebruiken, maar dat is redelijk beperkt. En we zijn ook aan het kijken of het sowieso nog nodig is om de usb open te laten staan, zodat het helemaal niet meer kan gebeuren.

RS: Ja en ben je dan nu samen met die afdeling kwaliteit aan het kijken hoe dit soort dingen aangepakt moeten worden?

Zorginstelling G: Ja, hoe we dit gaan borgen.

RS: Dus de echte implementatie daarvan moet nog een beetje komen?

Zorginstelling G: Ja dat zal begin volgend jaar volgen.

RS: En zijn jullie dan eigenlijk meer begonnen met de medewerkers meekrijgen of met…?

Zorginstelling G: Nou met de medewerkers meekrijgen sowieso en zorgen dat er technisch een aantal dingen georganiseerd en gedaan zijn en ja we moeten er nu echt naar toe zeg maar om ook het managementcommitment te hebben.

RS: die zitten in de Raad van Bestuur neem ik aan?

Zorginstelling G: Ja, die zitten ook in het managementgeheel zeg maar.

RS: Want hoeveel verschillende managers zijn er dan?

Zorginstelling G: Nou we hebben twee bestuurders en er zitten vier klantgroepen dus vijf directeuren daar zitten, die wekelijks overleg houden, dus daar moet het vandaan komen dan zeg maar.

RS: En dat is er op dit moment nog niet?

Zorginstelling G: Formeel nog niet nee. Ze weten zeker dat het de nodige aandacht heeft. Je hebt er continu discussie over, maar als je met de NEN en ISO bezig bent heb je echt managementcommitment nodig en het moet ook minimaal één keer in de maand op de agenda staan en vastgelegd worden wat daar besproken is en ook wat zijn de stukken die aangeleverd moeten worden. Dat moet volgend jaar echt ook gaan gebeuren zeg maar.

RS: Ja, dat het naar afdelingen ook echt wordt overgedragen zeg maar als er dingen zijn. Als er iets is of als er iets fout gegaan is bijvoorbeeld. Want je hebt nu bijvoorbeeld die Awarenessdingen worden die geëvalueerd?

Zorginstelling G: Ja, er komen sowieso vragen over van waarom iets is zoals dat aangegeven is of dat het eigenlijk veels te makkelijk is. Dan denk ik heel goed ik hoop dat dat voor iedereen geldt, want ja zo makkelijk is het dan toch ook weer niet. Maar we proberen daar wel van te leren zeg maar en je krijgt daar wel discussies over en dat is onderling, maar ook naar het management toe dat er dingen anders moeten of iets dan wel moet ja bijvoorbeeld al met Whatsapp. Het is makkelijk te vinden en bereiken voor thuis gebruik je het ook dus je weet allemaal hoe het werkt. Het is alleen jammer dat het van Facebook is en dergelijke en die kunnen er alles mee doen wat ze willen. Dus je moet het gewoon niet gebruiken en hetzelfde geldt voor mail, daar kan je ook geen dossiers mee versturen of informatie dat soort dingen mag ook niet.

RS: En wordt er op dit moment al in de organisatie geïnformeerd hierover?

Zorginstelling G: Ja, ja zeker. Ze weten ook dat het niet mag. Ik zeg niet dat het niet meer gebeurt, maar als het naar boven komt dat het gebeurt dan wordt er ook echt wel actie ondernomen en dan wordt er naar de afdelingen toegegaan om het te bespreken, maar goed zeggen dat iets niet mag vind ik altijd wel heel makkelijk. Je moet ook een alternatief aanbieden en daar zijn we mee bezig.

RS: Ja, dat maakt het natuurlijk lastig er moet wel een alternatief zijn. Dat zie je ook bij Google bijvoorbeeld.

Zorginstelling G: Nou ja bij Office 356 heb je bijvoorbeeld One Drive daar kun je eigenlijk hetzelfde mee als met Dropbox, je hebt Jemmer erin zitten. Dat is voor jouw organisatie net allemaal iets betrouwbaarder dan dat je dat bij de gratis versies doet. Er is niks gratis hè. Het is in ieder geval de informatie die jij aanlevert waarvoor jij betaalt en daar gebeurt van alles mee, dus daar moet je alternatieven voor verzinnen. Hoe wil je dat zoveel mogelijk afdichten, ook in je keten. Als je voorop loopt dan moet de rest ook nog mee hè.

RS: Want waar zitten dan lastige punten bijvoorbeeld om groepen te bereiken of om dingen door te kunnen voeren?

Zorginstelling G: Nou ja goed als je in een keten zit, dus het gaat van ziekenhuis naar zorginstelling naar de apotheek en die gegevens moeten wel rond zeg maar dus hoe doe je dat? Mail is dan best makkelijk zeg maar en vroeger werd er gefaxt, faxen gebeurt nog steeds, maar ook dat kan niet meer hè in ieder geval niet in de zin van bij de receptioniste waar alles binnen komt. Dat moet weer via een beveiligde printer, dus dat is allemaal wat strikter geworden. Maar ja als een huisarts zegt, ja leuk al die onzin maar ik doe er niet aan mee dan is dat wel de zwakste schakel zal ik maar zeggen. En ja die zijn er nog steeds, die het niet zo belangrijk vinden. Die gmail gebruiken bij wijze van spreken Dus ze zijn er allemaal nog.

RS: Want heb je hier ook nog artsen en doctoren en dergelijke?

Zorginstelling G: Ja er zijn ook artsen in dienst.

RS: Want ik hoor ook wel eens dat het EPD, het systeem waarmee dat bijgehouden wordt dat die voor een heleboel instellingen van een andere leverancier komt waardoor je ook heel vaak die vertaalslag niet kunt maken.

Zorginstelling G: Ja er zijn best veel leveranciers waar de dossiers in zitten en hoe ga je dat onderling communiceren?

RS: Ja, dat is ook een lastige.

Zorginstelling G: Ja, dat krijg je er allemaal gratis bij.

RS: Nou in ieder geval een belangrijke taak voor jou om er een beetje zicht op te krijgen. Nou in ieder geval hartstikke bedankt. Ik zal even checken of ik niet nog iets belangrijks ben vergeten. Zou vervelend zijn als je de resultaten niet met elkaar kunt vergelijken. Ik denk dat ik alles wel heb behandeld. Duidelijk verhaal dus dat is mooi.

5.8 Uitwerking interview zorginstelling H

Interview met twee FG's

RS: Eerst benieuwd hoe jullie op deze positie terecht zijn gekomen in deze organisatie?

H1: Ik ben hier terechtgekomen via de zorgadministratie. Dat is eigenlijk alle gegevensbewerking rondom de patiënt en vanaf eind jaren 80 heb ik ook al in de commissie privacybescherming gezeten en dat heeft ook altijd mijn warme belangstelling gehad. En ik ben tot drie jaar geleden manager geweest van de afdeling zorgadministratie. En dit is iets wat ik heel graag in mijn laatste fase in mijn carrière zou willen doen, echt weer de inhoud in, dus zo ben ik hier terechtgekomen. En het voordeel van mijn achtergrond is dat ik eigenlijk toch

wel vrij veel weet van de gegevensverwerkingen van deze organisatie en ook daarbuiten. Ik dacht dat ik redelijk wat wist over de wetgeving. Nou daar zit ik nu voor in een scholingsprogramma om dat helemaal ook goed in de vingers te krijgen. Het duurt drie jaar in totaal en je hebt gemiddeld elke zes weken een tentamen of een workshop. Je moet studiemateriaal bestuderen en dan krijg je een workshop en een tentamen en ik leer daar waanzinnig veel.

RS: De opleidingen verschillen wel erg: sommige cursussen duren bijvoorbeeld 10 dagen en dan krijg je al een certificaat.

H1: Ik ben er ook van overtuigd nu al dat het gemiddelde niveau van een functionaris gegevensbescherming te laag is. Domweg ook omdat het beroep eigenlijk niet gedefinieerd is en in de wet staat gewoon dat diegene voldoende kennis en vaardigheden moet hebben om die functie uit te voeren, maar daar komen we niet mee weg als je kijkt naar met wat voor vraagstukken wij te maken hebben en de kwetsbaarheid van de organisatie en de afwegingen die gedaan moeten worden dan is het toch wel van belang dat diegene redelijk geschoold is. Niet alleen in het wettelijke gedeelte, maar anderzijds moet je ook de afwegingen kunnen maken dus het ethische deel zal ik maar even zeggen. En dat betekent in feite dat je een afweging kunt maken tussen alle verschillende belangen die er zijn en dat je tot een afgewogen advies kunt komen. Dus dat is een subtiel spel.

RS: Ja en hoe ben jij bij deze functie gekomen (kijkt naar H2)?

H2: Ik ben hier 13 jaar geleden binnengekomen als kwaliteitsfunctionaris bij één van de onderzoeksinstituten en daar kwam ik erachter van 'hee wij moeten al onze onderzoeksprojecten bij het College Bescherming Persoonsgegevens melden'. Dat is niet heel erg handig, maar je kan ook melden bij de functionaris gegevensbescherming van de organisatie en sindsdien ben ik FG voor het onderzoeksinstituut en sinds een jaar of drie vier ben ik dus functionaris gegevensbescherming van al het onderzoek en onderwijs heb ik er ook bij gekregen.

H1: Onderzoek en onderwijs heel eigen karakter, heeft eigen risico's. En ik doe dan zorg en de s-voering.

RS: Dus jullie zijn dan twee FG's en zijn hier nog andere FG's?

H1: In feite niet formeel aangemeld maar we vormen in totaal een team van vier personen. Dat zijn drie FG's bij elkaar die dat niveau en de kennis hebben en één iemand die moet ons een beetje bij de les houden en die is de documentalist.

RS: En hoe valt dat dan in de rest van de organisatie? Valt dat onder een afdeling of staat dat op zichzelf?

H1: Wij vormen een team. H2 zit in de divisie waar onderzoek plaatsvindt en ik zit bij bestuurlijke en juridische zaken, dus dat is het bureau van de Raad van Bestuur, maar ik heb daar natuurlijk een onafhankelijke positie in. Ik ben toezichthouder, want het zijn wettelijke taken voor ons tweeën. De belangrijkste zijn denk ik: toezichthouden, adviseren en awareness. Dat zijn onze kerntaken.

RS: En je hebt natuurlijk privacy en je hebt de bescherming van persoonsgegevens. Hoe staan die twee tot elkaar in verhouding volgens jullie?

H1: Hoe bedoel je?

RS: Nou het wordt natuurlijk best wel vaak door elkaar gebruikt privacy en de bescherming van persoonsgegevens maken jullie daar een onderscheid in?

H1: Nou wij zien privacybescherming dat is eigenlijk de hele Wet Bescherming Persoonsgegevens en alles wat daarbij hoort.

H2: Onze afdeling heet eigenlijk privacybescherming en informatiebeveiliging. Dat loopt enorm in elkaar over.

H1: Maar wij zeggen dat heeft met elkaar te maken, want informatiebeveiliging dat is eigenlijk in feite de uitwerking van artikel 13 dat je technische en organisatorische maatregelen neemt. En voor ons is voor de

informatiebeveiliging de NEN7510 norm en die willen we dan geïmplementeerd hebben en daar willen we als gecertificeerd zijn. We werken dus ook in een netwerk met mensen die zich daarmee bezighouden, dus informatiebeveiliging wat veel technische kanten heeft, samen met de technical security officer van de ICT-afdeling, maar ook met hoofd veiligheid als het gaat om fysieke gegevens en dergelijke.

RS: Ja dan kun je de mensen die je nodig hebt er via die weg bijhalen.

H1: Eigenlijk is het netwerk nog groter, want wij werken met z'n vieren samen maar we werken ook met de bedrijfsjuristen samen, met de gezondheidszorgjuristen werken we samen, Hoofd Veiligheid en met de technical security officers van de ICT-afdeling, daar vormen we eigenlijk een eenheid mee.

RS: Oké dat is best wel breed.

H2: Heel breed, maar de problematiek is ook breed.

RS: Ja, zeker, dat klopt. En als jullie dan beleid of iets dergelijks willen opstellen gaat dat dan via jullie of komt dat vanuit de Raad van Bestuur?

H1: Wij zijn wel de trekkers, maar wij mobiliseren onder andere natuurlijk dat hele netwerk en de rest van de organisatie en we zorgen ook dat we de opdracht hebben in feite ook van de Raad van Bestuur, maar wat eruit komt, dus het informatiebeveiligingsbeleid daar staat natuurlijk de Raad van Bestuur vierkant achter en wij doen alleen maar mensen bij elkaar brengen en zorgen dat het op papier komt.

RS: Ja, want hoe hebben zij dit thema in beeld, zijn zij daar veel mee bezig?

H1: Ja, volledig

H2: Zij zijn daar niet zo blij mee, maar dan heb je het over de datalekken.

H1: Klein stukje historie. We hebben bij deze instelling een aantal jaren terug een incident gehad, waarbij onze instelling op een behoorlijke manier de privacy geschonden had van patiënten. Dat is een rel geworden van jewelste. Maar als je dat even doortrekt naar de Raad van Bestuur, die dat ook opgevallen is en daarmee door dat incident is privacybescherming bij deze instelling hoog op de prioriteitenlijst gezet. Daarom zijn wij er ook daarom zijn wij ook benoemd en geregistreerd en weet ik het allemaal. De Raad van Bestuur heeft dit als vast onderwerp en een van de leden van de Raad van Bestuur heeft dit ook in zijn portefeuille en daar hebben wij ook regulier overleg mee en wij moeten ook op regelmatige basis rapporteren aan de Raad van Bestuur hoe de zaken ervoor staan. Daarbovenop worden we twee keer per jaar door externe audits ge-audit.

H2: Maar dat gaat meer over de informatiebeveiliging.

RS: Ja, maar het is ook belangrijk natuurlijk dat het door de Raad van Bestuur een beetje gedragen wordt om het in de organisatie door te voeren in ieder geval. En hebben jullie ook een communicatieafdeling?

H2: Ja.

RS: En als er dan bijvoorbeeld iets moet gebeuren op het gebied van awareness?

H1: Die heeft een prachtige site gemaakt voor de privacybescherming en informatiebeveiliging. Met name ook over social media waar in dit geval nogal wat risico's aan verbonden zijn. Alle uitingen die gemaakt worden in het kader van awareness, rondom privacybescherming of informatiebeveiliging lopen via een vast contactpersoon op de afdeling communicatie die zit ook in de commissie privacybescherming en informatiebeveiliging.

RS: Oké dus via die weg wordt hij er dan in betrokken. Kennen jullie dan bijvoorbeeld ook de 'ZEKER' campagne van de NVZ?

H1: Daar hebben we ook aan meegedaan gedeeltelijk. Er zijn een aantal berichten via onze reguliere media het huis in gegaan om de privacybescherming te bevorderen op basis van die campagne. We hebben niet volledig met die campagne meegedaan. Ik weet niet meer precies wat wel en wat niet.

H2: Nou ja de voorbeelden die ze hadden van bijvoorbeeld met zo'n middag zetten ze een boef erin tussen de wachtkamer. Dat vond ik niet zo aansprekend.

H1: Nee, het was niet zo aansprekend. We hebben wel meegedaan, alleen we hebben er wat eigen ideeën aan gegeven.

RS: Ja, dat zie je wel vaker gebeuren. Ze leveren natuurlijk een algemeen pakket waar je keuzes in kan maken.

H1: Nee, je bent dom als je niet meedraait, want er wordt ook wel gewoon landelijk aandacht aan besteed en als je dan niets doet in je eigen huis, dat is niet best. Maar die campagne werd door ons niet als heel erg adequaat bestempeld.

RS: Ja, want hebben jullie bijvoorbeeld ook die zekertest ingezet in jullie organisatie?

H2: Nee.

RS: Oké ja dat was zo'n test waar je mee kon zien hoe bewust je omgaat met persoonsgegevens als medewerker, alleen daar waren dan wat conclusies uitgetrokken van de NVZ uit dat medewerkers goed omgingen met persoonsgegevens. Dus ik zag dat resultaat en ik dacht vanuit mijn onderzoeksachtergrond: klopt dit wel? Maar dit was natuurlijk eigenlijk een awarenesscampagne, dus dan stel je vragen om awareness te creëren dat is iets anders dan wanneer je vragen stelt om onderzoek te doen.

H2: Ja, dat je sociaal wenselijke antwoorden krijgt.

RS: Bijvoorbeeld wat zou je doen als er een computer open staat, log je die dan alsnog uit etc. Maar daar hebben jullie dan niet aan mee gedaan.

H1: Wel aandacht aan besteed in die periode via die artikelen en dergelijke maar niet specifiek die test.

RS: En wat doen jullie dan bijvoorbeeld aan awareness?

H2: Dat hangt er ook een beetje vanaf over welk terrein je het hebt. Wij zijn een redelijk uitzonderlijk UMC, dat ik er namelijk ben. Zoveel aandacht voor research is er niet. En voor een deel is het allemaal in het research ingebakken. Een heleboel van ons onderzoek gaat langs de medische ethische toetsingscommissie, ken je die?

RS: Ja.

H2: En deze toetsingscommissie kijkt is iets WMO(Wet Maatschappelijke Ondersteuning) of is iets niet WMO. Als het WMO is dan gaat het door een heel circus heen en niet WMO dan is het bij de meeste UMC's ga je gang maar. Hier kijken wij dan erg sterk naar de privacy. En daarin creëer je ook een stuk awareness. Bijvoorbeeld het woord anoniem ben ik aan het uitbannen. Dan staat er: uw gegevens zullen anoniem zijn. Nee, wij weten wie die persoon is dus dat kun je niet zo opschrijven. En dat is ook een stukje opvoeden van de organisatie wat daar ook in zit, dat zit er eigenlijk structureel in.

RS: En als je dan bijvoorbeeld denkt aan wat meer communicatiemiddelen, worden die ingezet bij medewerkers in de organisatie?

H1: Nou wat we op dit moment doen: we hebben sowieso van die posters, do's en don'ts die zie je nog steeds hangen, we doen gebouwrondes. Iedere twee maanden doen we zo'n gebouwdeel en dan leggen we een soort kaarten neer met smileys met achterop wat wel en niet kan. Of afkeurend met andere woorden dit is niet in orde wat ik hier tegenkom. We merken dat dat een heel sterk awareness bevorderend effect heeft, want als we ergens een ronde gedaan hebben, worden we meteen heel vaak gebeld van waarom dat zo is. En daarnaast

zie je die kaarten her en der. We hebben op de site, we hebben een eigen site of eigenlijk twee één voor privacy en informatiebeveiliging, maar ook voor bewust met social media omgaan. Dat is voor ons namelijk ook een bedreiging van de privacy van medewerkers en van de patiënten kan dat zijn. We hebben als mensen binnenkomen dan worden ze via een obligaat praatje of in ieder geval is dat geautomatiseerd worden ze meegenomen wat privacybescherming, informatiebeveiliging en beroepsgeheim betekent.

RS: Ja, dus dat is voor de externe kant voor de patiënten?

H1: Nee, dat is voor intern dat is voor medewerkers.

H2: Nieuwe medewerkers.

RS: Oh als ze hier binnenkomen, als in binnenkomen in de organisatie.

H1: Nou daarnaast wat we ook wel doen aan awareness, hebben we regelmatig als er een issue is correspondentie met afdelingen. Als er iets belangrijks is zoals een datalek of ik noem maar wat dan komt dat ook in ons weekblad. Als er ernstige incidenten zijn bijvoorbeeld dat betekent ook dat we er aandacht aan besteden van 'héé we zien dit ook vaak terugkomen dus dan komt er weer een artikeltje om de awareness te bevorderen'. Alles bij elkaar genomen onder de streep vinden we het volstrekt onvoldoende, want hier in de organisatie wordt gebrek aan awareness als een heel groot risico gezien dat merken wij ook als wij die incidenten afhandelen: hoe halen ze het in hun hoofd om dit gedaan te hebben weet je wel. En dat komt toch omdat mensen nou het begint bij awareness als je je bewust bent van iets dan ga je daarnaar handelen dus dat is fase 1. Nou volgens mij hebben ze die fase 1 nooit doorlopen. En we willen nu ook dat gaan we nu ontwikkelen, e-learningmodules op het gebied van privacybescherming en informatiebeveiliging die verplicht worden voor alle medewerkers maar wel wat meer toegesneden op de groepen, want informatiebeveiliging en privacybescherming betekent iets anders voor mensen in de zorg zoals dokters of verpleegkundigen, maar het betekent ook weer wat anders voor mensen die bij ondersteunende afdelingen werken of voor onderzoekers. Dus op die manier, als je dat niet doet dan worden je bevoegdheden ingetrokken, zo willen we eigenlijk de awareness erin stampen.

RS: Ja, dus dan moeten ze wel in ieder geval die module doen, want nu komen ze bijvoorbeeld een artikel tegen of iets dergelijks, hebben jullie ook een intranet?

H2: Ja, we hebben ook een intranet en ICT zet daar bijvoorbeeld ook regelmatig berichtjes op als er weer ransomware is of iets anders, maar dat wordt slecht gelezen.

H1: Maar de effectiviteit daar hebben wij grote twijfels over.

RS: oké.

H1: Als we kijken naar de incidenten die er dan zijn die we afhandelen, dat wij elke keer ons afvragen van 'hoe is dit nou mogelijk?'

RS: Want op welke manier worden dan de verschillende groepen benaderd, wordt daar nu al onderscheid in gemaakt?

H1: Nee. Dat is wel een goede wat je vraagt nu. We hebben ook in het kader van de awareness een zogenaamde contactpersonenbijeenkomst. Eigenlijk in feite heeft iedere afdeling, als ze allemaal zouden komen zou het heel mooi zijn, een contactpersoon privacybescherming en informatiebeveiliging. Daarvoor organiseren we kwartaalbijeenkomsten om allerlei onderwerpen te bespreken. Dat zijn eigenlijk onze ambassadeurs op de afdelingen. Nou je voelt al wel aan dat wordt op verschillende manieren ingevuld. De één is heel actief en de ander die gaat erheen die gaapt drie keer eet zijn broodje op en gaat weer terug.

H2: Ja, dat hangt ook van de aanpak af. Waar ik wat meer heen wil is dat we ze een soort pakketjes aanbieden. Bijvoorbeeld een powerpoint met een vraagstelling erop, twee sheets die in je werkoverleg gebruikt kunnen worden om op de afdeling te bespreken.

RS: Ja dus dat het wat vaker terugkomt maar misschien wel in een lichtere vorm?

H2: Lichtere vorm en praktisch.

RS: Ja.

H2: Waar ik de meeste vragen over krijg is 'ja maar wat moet ik dan? Hoe kan ik het dan veilig versturen?'

H1: Een veel voorkomende vraag.

RS: Ja, dat zijn natuurlijk ook lastige punten.

H2: En anders mag dit? En dat is een andere vraag waar ik meestal mee zit: mag dit?

H1: Ik merk wel dat als ik op de afdelingen ben, daar hadden we het vorige week ook over, dan zijn die zorgverleners zich allemaal heel erg bewust van het beroepsgeheim. Met hoofdletters en drie strepen erachter dat is er wel ingepeperd. Dat is natuurlijk op zich al heel belangrijk dat ze zich daar bewust van zijn. Maar de bepalingen die voortvloeien weer uit de Wet Bescherming Persoonsgegevens die kennen ze weer niet en de privacyaspecten zoals die opgenomen zijn daar weten ze ook betrekkelijk weinig van.

RS: Ja, maar je zou wel zeggen dat ze dan al de bewustwording hebben.

H2: Ja, zeker die hebben ze, maar op een gegeven moment heb je, dat vind ik wel een heel mooi voorbeeld, waar je dan specifiek in het research domein tegenaan loopt. Kijk artsen vragen altijd naar een geboortedatum en een naam om er zeker van te zijn dat je de juiste patiënt voor je hebt en dat moet ook. Maar op het moment dat je nu zegt van we gaan nu onderzoek doen dan is het eigenlijk al not done. Dan mag dat eigenlijk alleen maar gecodeerd dat je niet meer meteen weet wie het is. En die omschakeling die moeten velen nog maken, dus dat je dan dus niet naar een geboortedatum moet vragen want die heb je ook helemaal niet nodig. Heb je niet aan een leeftijd genoeg of nog beter aan een leeftijdscategorie?

RS: Ja, en dat is voor de mensen achter de balie wel relevant natuurlijk voor in de zorg om te weten wie je voor je hebt, maar voor onderzoek niet.

H2: Ja, voor onderzoek niet. Daar is het ook wel belangrijk, maar daar valt een vergissinkje, ja dat kan wel pijnlijk zijn voor het onderzoek maar ja de patiënt wordt er over het algemeen niet zieker op.

RS: En waar zitten dan lastige punten om die groepen te bereiken?

H1: Nou lastige punten om die groepen te bereiken. Op zich kun je die groepen prima bereiken alleen je moet zorgen dat je hun aandacht krijgt. Hè want iedereen is hier natuurlijk heel erg druk en logisch ook dat is echt gewoon patiënten, onderzoek en onderwijs. Dit is natuurlijk iets wat erbij komt. Ze werken natuurlijk in een wetgevend kader op allerlei gebieden. Ze hebben het over corporate governance en huiscircuit en budgetten en weet ik het allemaal daar zit ook een stuk privacy en informatiebeveiliging bij, dus je moet zien dat je op een of andere manier met begrip voor waar die mensen al dan niet functioneren en waarvoor ze hier zijn. Moet je proberen op een gepaste manier aandacht hiervoor te krijgen, want de risico's zijn wel steeds groter. Dus dat nemen we dan wel mee. Wat ook belangrijk is, is toon het top, nou die hoogste top is zeker wat betreft privacy en informatiebeveiliging bij de les. Dat stralen ze ook uit. Dat is al één randvoorwaarde. Maar we spreken nu ook duidelijk de hele lijn aan dus afdelingshoofden en werkplekmensen op hun verantwoordelijkheid daarin. Als je het niet goed doet, dan kunnen dit de consequenties zijn. Dat vertellen wij aan die mensen. Als je daar vanuit onze rol als FG's consequent in bent, dat die mensen het ook echt begrijpen en dat het tot hun hersenen doordringt dat ze zorgvuldig moeten handelen omdat er anders ernstige consequenties kunnen zijn dan gaat het ook een stuk beter merken we.

RS: Ja, want zijn er op dit moment al maatregelen als mensen zich er niet aan houden of bijvoorbeeld een melding niet doen van een datalek?

H1: Nou dat is wel een goede van je. Onder andere doen we nu aan login-opvolging. Met andere woorden: 'heb je rechtmatig toegang gekregen?' Er is nu een complete brief in de maak, die naar iedereen gaat die vertrouwelijke gegevens moet raadplegen, die krijgen het op de deurmat. Daar staat ook in inderdaad dat er spelregels zijn en dat als ze zich daar niet aan houden dan kan dat rechtspositionele consequenties hebben, zoals een disciplinair gesprek tot en met ontslag. De Raad van Bestuur zegt: we gaan hieraan echt consequenties verbinden.

RS: Ja, dus de Raad van Bestuur heeft die risico's in ieder geval goed in beeld, want wat zien zij dan als risico's voor deze specifieke instelling?

H1: Heel goed. Nou natuurlijk het onrechtmatig raadplegen van gegevens. In zijn algemeenheid geldt hè als je kijkt naar de risico's waarvan ze zeggen: ojee daar komt ellende uit. Op nummer 1 staat met stipt het gebrek aan awareness waardoor mensen in kennis gehinderd fouten maken en daardoor incidenten veroorzaken. En waarvoor wij eigenlijk nog het meest beducht zijn dat is reputatieschade.

RS: Ja.

H1: Dat is voor zo'n organisatie, een gezondheidsorganisatie, is dat het allerbelangrijkst.

RS: Ja, want hebben jullie dan bij dat incident daar dingen van gemerkt dat er dingen veranderden in de reputatie?

H1: Ja er is een enorme reputatieschade aangericht in die tijd. Dus daar zijn ze zich heel erg van bewust: 'straks word ik door mevrouw Tweebeeke onder handen genomen' Want onze Raad van Bestuur is toen natuurlijk afgebrand.

RS: Ja dus dat hebben ze dan heel goed in de picture zeg maar.

H1: Wij zijn ook opportunistisch hoor. Als er een incident is dan kijken wij wat er ook alweer op ons lijstje staat en dan oja dat hoort daarbij en dan meteen zetten we dat erin als advies naar de Raad van Bestuur, want we hebben een vaste afhandelprocedure. Dus wij maken elk incident dat een beetje omvang heeft, daar maken wij misbruik van om meteen de Raad van Bestuur te laten stempelen van daar moet wat gebeuren.

RS: Ja, om dan je lijstje erbij te pakken en te zeggen van 'oja zie je wel er gaan daar dingen mis op die manier'. En in hoeverre denk je dan dat communicatie een rol zou kunnen spelen in het inperken van de risico's?

H1: Nou het feit dat het ook benoemd is. We hebben net een managementreview geschreven naar de Raad van Bestuur. Dan kan de Raad van Bestuur zich een oordeel vormen hoe het hier op dit moment is ten aanzien van informatiebeveiliging, maar dat hangt samen met privacybescherming natuurlijk. En daar staat gebrek aan awareness op nummer één, dus communicatie is natuurlijk het allerbelangrijkste.

H2: Maar wat jij hier noemt: knelpunt. Nou één van de knelpunten is de tijd die wij zelf erin kunnen steken. Het is iets dat structureel aandacht nodig heeft en het lukt ons nog niet helemaal om daar helemaal genoeg capaciteit in te steken.

RS: Nee, dus eigenlijk zou er wel wat meer ruimte voor mogen komen of nog iemand aangesteld moeten worden?

H1: Nou dat gaat niet gebeuren, maar je moet natuurlijk proberen je netwerk groter te krijgen, mensen die daarmee bezig zijn. Dat is het enige wat op dit moment tot capaciteitsuitbreiding zou kunnen werken, maar ik zou zelf eerder benoemen: weet je communicatie is echt een heel moeilijk vak eigenlijk om dat goed te doen en dit is iets: je kan niet zeggen we gaan één keer communiceren en dan weet iedereen het. Nee, dit heeft een soort permanente aandacht nodig en weet je het is net zo als dat je iedere avond boerenkool zou eten, dat zou heel erg gaan vervelen. Zorg dat je telkens wel iets op een andere manier doet, waardoor je mensen blijft aanspreken. En wij zijn natuurlijk vanuit ons vak heel sterk gericht op de inhoud en je wilt vanuit de inhoud je

boodschap kwijt, maar omdat je zoveel kennis hebt van het vakgebied, schiet zo'n boodschap vaak ook zijn doel mis natuurlijk.

RS: Ja dat is een beetje het voorbeeld van die mensen die met drie gapen bij de verhalen zitten.

H1: Ja natuurlijk, ja. We zijn natuurlijk heel trots dat we overal van die do's en dont's posters ophangen, maar ja ik weet zelf ook wel dat de effectiviteit daarvan beperkt is. We doen het alleen voor een auditer eigenlijk, een externe auditer, van kijk daar hangt ie. Nou top je hebt je in ieder geval aan die norm heb je voldaan. Maar eigenlijk willen wij wat onze visie daarop is wij willen eigenlijk echt effect bereiken. De Raad van Bestuur wil ook echt effect de Raad van Bestuur geeft de opdracht om echt effect te hebben: 'wij willen geen papieren tijgers'. Ik vind zelf die creativiteit om telkens op een goede manier mensen te bereiken, dat vind ik het allermoeilijkste.

RS: Ja, want wat zijn dan bijvoorbeeld strategieën waarvan je merkt dat het nu juist wel werkt of juist niet?

H1: Nou strategieën, als je praat over de awareness zien wij wel dat de datalekken dat dat ons enorm helpt.

H2: Maar dat zijn herkenbare voorbeelden, want heel vaak wat in die wetgeving staat dat is eigenlijk alleen te abstract. En dan maak je al een heleboel vertaalslagen naar de praktijk, maar dan nog blijft het moeilijk. Dus voor een deel is het: hoe verpak je onze boodschap in iets waar mensen wat van begrepen hebben en wat blijft hangen?

RS: Ja.

H2: En vaak helpt het inderdaad gewoon als je een mooie casus hebt waaraan je het kan ophangen, want dan herkennen ze het en dan kom je erin.

H1: Sowieso hè nog wel een belangrijk aspect dat wil ik dan nog wel noemen. Als je kijkt naar de FG's, die zijn heel erg goed in die wet en de interpretatie van die wet en dat vind ik echt onvoorstelbaar en dat vind ik heel knap ook, maar het gaat er natuurlijk om. Je kan het beter ietsje minder weten, maar juist in het communiceren erover ook face-to-face, met mensen over praten, zorgen dat het op de agenda staat, jezelf in feite ook een beetje opdringen hè maar dan op een leuke manier, dus erover communiceren is het allerbelangrijkst. En je denkt vaak over communicatie met plaatjes, posters en al dat soort dingen en filmpjes, maar het communiceren dat de FG's dat doen, met de leiding, met het management, met de werkvloer. Erheen gaan is nog veel belangrijker. Het uitspitten van de wet en dan een hele grote Excel te maken dat je precies weet waar het verschil zit en wat er dan voor maatregelen genomen moeten worden, daar bereik je het niet mee.

RS: Want worden er dan ook casussen besproken als er dingen voorvallen in de organisatie of alleen bij de betreffende afdeling?

H1: De incidenten sowieso. Dat is ook verplicht. Afdelingen moeten ook verplicht melden en die vraag ik ook naar audits dan, maar sinds we de Wet Meldplicht Datalekken hebben, hebben we wel daadwerkelijk incidenten waar ook een hele hoop mensen mee aan de gang gaan en die mensen worden ook verwacht waar de incidenten ontstaan dat ze er wat mee doen en daar worden ze ook op aangesproken. En wat wij nu willen doen en dat zei jij ook vorige week dat we deze incidenten ook gaan gebruiken als voorbeelden om de incidenten ook sprekend te maken.

RS: Ja, want merken jullie dan ook in de organisatie veranderingen sinds de wet is ingevoerd?

H2: Ja, er is natuurlijk ook meer aandacht aan gegeven. Ik merk zelfs bij mensen die het eigenlijk al zouden moeten weten die denken er dan niet aan. Die weten het eigenlijk wel, maar die betrekken het dan niet op hun eigen situatie. Concreet voorbeeld: iemand was met een online vragenlijst bezig en realiseerde zich opeens bij een vragenlijst besteedt je dingen uit, dus hoort daar een bewerkersovereenkomst bij. Die was daar eigenlijk

ook wel van op de hoogte, maar voor haar eigen onderzoek viel op een gegeven moment pas het kwartje van oh ja dat is waar ook. Op een gegeven moment moet je daar dus iets voor gaan regelen.

H1: Wat we ook, dat wil ik toch wel even noemen als het gaat om communicatie en awareness en dergelijke. Wij zeggen ook van privacybescherming en informatiebeveiliging moeten onderdeel zijn van de reguliere bedrijfsvoering. Dat iemand dat een beetje apart zit te oreren vanuit een ivoren toren dat werkt gewoon niet. Wat we nu aan het doen zijn is een aantal zaken. Je hebt de plan – do – check – act cyclus, dat is de sturende manier van deze organisatie waaraan eigenlijk het hele lijnmanagement aan deelneemt en daar willen wij eigenlijk ook als het ware een normaal onderdeel van zijn. Onder andere is het zo dat hebben we bijna bereikt: dat we gewoon gaan deelnemen aan de reguliere interne audits hier, dus privacy en informatiebeveiliging wordt onderdeel daarvan, dus tegelijkertijd met patiëntveiligheid en informatiebeveiliging wordt dan ook getest. Oja, één dag behandelen we al deze aspecten.

H2: En als we dan vergelijken met andere organisaties die beperken dan de privacy tot de zorg, maar wij pakken dan gelijk het onderzoek mee op zo'n afdeling. Dat loopt ontzettend door elkaar heen namelijk.

H1: Een ander punt waarop we dat willen bereiken, daar zijn we ook wat laat mee, is het integraal risicomanagement, dus patiëntveiligheid, financiën, gebouwen. We hebben nu ook geregeld dat we ook onderdeel zijn van het risicomanagement van deze instelling.

RS: Ja, dus dat er ook risico-inventarisatie en dergelijke gedaan kan worden?

H1: Ja, dat doen wij nu al hè risico-inventarisatie, maar dat moet natuurlijk een onderdeel zijn van de integrale bedrijfsvoering. Waarom zijn het anders risico's? Het is gewoon weer een risico. Dus onze visie is ook maak het onderdeel van de integrale bedrijfsvoering. We zijn daar acties voor aan het ondernemen dat dat daadwerkelijk gebeurt. Je moet altijd een soort lange termijnvisie hebben, want als je dan kijkt naar hoe is het ideaal geregeld als je dan wil dat het op een zo'n onderdeel ideaal geregeld is zoals het beschreven staat en in de norm opgenomen staat dat is een heilloze weg dan verlies je meteen je geloofwaardigheid. En dan ben je in plaats van dat je een stapje vooruit maakt, ben je er tien achteruit, want mensen gaan je ook vermijden, dus je moet eigenlijk ook proberen een stap te maken waarvan je zegt ja dit is het nog helemaal niet, maar het is een stap voorwaarts. Dan weet je oja, nu deze stap en volgend jaar die stap. Dus je moet als het ware een langetermijnvisie hebben waar je uiteindelijk wilt komen. Nou heb ik nog nooit meegemaakt in mijn leven dat ik mijn doel bereikt heb dat blijft toch altijd voor zich uit bewegen, maar je moet wel een organisatie als het ware meenemen.

RS: Ja, want hebben jullie dan een procedure ingericht bijvoorbeeld voor de datalekken?

H1: Nou die werkt als de beste.

RS: Want wat voor procedure hebben jullie daarvoor opgesteld? Is er bijvoorbeeld een intern meldpunt waar de medewerkers terecht kunnen?

H2: De praktijk leert dat wij meestal gebeld worden of er komt een mailtje binnen of het komt via ons meldsysteem, maar het meeste is gewoon rechtstreeks contact met ons.

H1: Ja, of mensen rennen m'n kamer in. Nog even over de signalering, want dat is eigenlijk het allerbelangrijkst, wat hebben wij ingericht voor de signalering? Dat is vrij uitgebreid. Doen we even op volgorde: er kan gebeld worden, een nummer gewoon. We hebben dat mensen persoonlijk binnen kunnen komen. We hebben een meldsysteem daarin staan ook een aantal vragen naar een datalek. We hebben omdat datalekken ook op allerlei manieren kunnen binnenkomen ook verloren pc's en weet ik wat het allemaal zijn. Receptie of beveiliging neemt meteen met mij contact op als er sprake is van een gestolen laptop of een gevonden laptop of iets anders in de harde sfeer. Daarnaast kunnen ook datalekken binnenkomen via social media. Voor ons wordt permanent social media in de gaten gehouden wat erover gezegd wordt, dus zodra er sprake is van een melding of iets wat een datalek zou kunnen zijn, dat is nog nooit gebeurd trouwens.

RS: Nee, want daar vroeg ik me dan ook van af wat stel je je daarbij voor? Dat een medewerker of een patiënt iets online zet van ik heb dit meegemaakt of iets dergelijks?

H1: Allemaal. Of je moet het ook anders zien.

H2: We hadden zoiets gehad er stonden röntgenfoto's van iemand die stonden op internet. Dat klopte allemaal, maar dan kan je zeggen van hee.

H1: Maar ook klagende mensen van: nou m'n gegevens lagen daar en daar en hoe vind ik dat nou hè? Dus dan gaan mensen in hun omgeving via social media dingen zeggen. Daarnaast krijg ik ook iedere dag worden alle andere media, de formele media, gescreend op onze instelling. Die kijken iedere dag na of het een artikel zou betreffen waarin iets over het uitlekken van gegevens staat. Nou zijn we een tijdje geleden naar aanleiding van zo'n uitzending ook getipt door een collega dat er mogelijk sprake zou zijn van een datalek. Ik vond het te ver gaan en heb er niks mee gedaan, hij vond van wel. Maar goed dat is ook mijn beoordeling. Dat is de voorkant hè dus die wordt dichtgetimmerd.

RS: Als mensen ook daadwerkelijk gaan melden natuurlijk.

H1: Nou dus een hele korte procedure, tak tak tak tak, voor de afhandeling.

H2: Je mist nog één dat is de afdeling ICT.

H1: Oja ICT, sorry een hele belangrijke, de helpdesk waar ook natuurlijk van alles binnen kan komen en die melden het ook direct bij ons als er sprake is van een ernstig datalek, zoals malware of gegevens vernietigd dat is een datalek. Dan doen wij de eerste beoordeling en indien het een ernstig incident is dan nemen wij meteen contact op met de secretaris van de Raad van Bestuur dan vind er een beoordeling plaats en dan wordt gekeken of we dat in een kleine setting kunnen afhandelen. Dat betekent dat wij toetsen aan de wet en kijken of we melding moeten doen aan de AP en of betrokkenen geïnformeerd moeten worden en dergelijke en op die manier geven wij dan een advies en dat neemt de Raad van Bestuur over of niet en dan zorgen wij dat het uitgevoerd wordt, maar bij een ernstig incident, met andere woorden veel gegevens, mogelijk ook imagoschade, dat hebben we eigenlijk twee keer gehad maar daar hebben we één lek van gemaakt dan wordt het hele circus opgetrommeld. Iemand uit de Raad van Bestuur wordt de voorzitter van de beheersgroep. Daar zit ook de directeur Communicatie en daar zit de voorzitter van de commissie privacybescherming in en daar zitten wij in en daar zit de directeur ICT bij en de technical security officer die kennis heeft van de harde informatiebeveiliging, dus heel technisch.

H2: En verder mensen die dan nodig zijn van de afdeling.

H1: En dan komen we afhankelijk van de ernst: één of meerdere keren per dag bij elkaar zal ik maar zeggen. En dan wordt daar netjes verslag van gemaakt en we bouwen een dossier op. De procedure is eigenlijk heel kort en krachtig. Het zijn eigenlijk maar drie velletjes en dat is ook eigenlijk de kracht van de procedure: iedereen weet meteen wat hij moet doen en wij zijn eigenlijk degenen die dan het proces sturen. Dat is een hele belangrijke rol die we hebben. Wij zijn toezichthouders en adviseurs he, dus vanuit die rol doen we dan ook dat we adviseren wie wat moet vinden, besluiten, afwegen enzovoort, dus wij regisseren dat.

RS: Dus je gaat dan naar de secretaris Raad van Bestuur om het aan te geven en dan beoordeel je of het voor die grote groep gaat of voor een kleinere setting.

H1: Ja, maar altijd als er sprake is van een door ons gedetecteerd datalek dat beoordelen we eerst, dan beoordelen we vervolgens of we de AP inlichten en de betrokkenen moeten informeren. Dan volgt er altijd een advies van ons tweeën want we reviewen mekaar ook. En dan gaat dat advies, ons gezamenlijke advies altijd naar de Raad van Bestuur naar een vast persoon, één voor de zorg en één voor onderzoek en onderwijs. En dan nemen ze het al dan niet over. En dan geven ze het terug en dan zorgen wij dat het als zodanig afgehandeld wordt.

RS: Ja, maar ze kunnen er ook voor kiezen ook om het niet over te nemen en wat gebeurt er dan?

H2: Dat hangt er vanaf wat er is. Meestal is het advies wel of niet melden bij AP of wel of niet melden bij de betrokkenen. En vaak komen er ook wel maatregelen dus die stellen we ook voor.

RS: Ja, dus het is vrij concreet ingevuld al.

H2: Het is heel concreet ja.

RS: En want zij zijn uiteindelijk wel dan degene die mogen beslissen of iets gemeld wordt of niet?

H1: Ja, zij moeten, wij mogen niets wat dat betreft, zij moeten. We hebben een soort standaard rapportage staccato, de feiten. En dan krijg je soms een beetje context erbij en dan beoordelen we is het een datalek ja of nee? en dan een stukje wet. En dan moet de betrokkene geïnformeerd ja of nee? De AP?

H2: Afwegingen en daar staan onze aanbevelingen dan. Want ze moeten heel snel beslissen. En daarmee stel je je ze daartoe in staat.

RS: En hebben jullie dan ook al een keer contact opgenomen met de Autoriteit Persoonsgegevens? Niet perse een melding gedaan, maar misschien informatie ontvangen?

H1: Ja, we hebben wel informatie gevraagd niet over datalekken, maar in het kader van de interpretatie van de beleidsregels. Hoe heet dat ook alweer medisch dossier van zieke medewerkers. Nou ja in april hebben we die vraag gesteld en we hebben eind vorige maand pas antwoord gekregen eigenlijk, nog niet eens officieel maar officieus. En dat duurt heel lang en we merken wel dat dat advies van de autoriteit persoonsgegevens dat is typisch ivoren toren advies, want het sluit niet aan bij eigenlijk de praktijk. Het advies van de autoriteit persoonsgegevens van onze kant denken wij dat zij dan ook moeten kijken naar de context waarin dat advies als het ware omgezet moet worden in werkbare processen. Duurt erg lang. We kregen ook vorige week toen werd jij benaderd een paar weken geleden over een datalek van een patiënt en dat de AP dacht van welk datalek zal dit overgaan?

H2: Ja, we hebben meerdere datalekken gemeld.

H1: Ja een stuk of zes denk ik ook hè. Ja want we moeten ook weer verslag erover uitbrengen natuurlijk.

RS: Ja want dan heb je dus gemeld en dan krijg je een vraag van de autoriteit?

H2: Ja dat dacht ik maar dat ging over iets heel anders dat ging over een medewerker die had geklaagd over de procedure als je je wachtwoord vergeten bent, dan wordt het BSN gebruikt en daar had dan iemand over geklaagd. Gelukkig hadden we het zelf ook al gedetecteerd en hadden we het opgelost. Ergens in de zomer is die procedure geweest maar de klacht was al van voor de zomer.

H1: Kortom ze zijn traag en als er advies gevraagd wordt is onze ervaring dat het advies nog niet aansluit bij de praktijk.

H2: Nou dat het te ver weg staat, ze gaan puur van het juridisch theoretische uit.

RS: Dus het is eigenlijk een beetje afstandelijk. Hebben jullie ze toevallig al een keer gesproken of gezien?

H1: Nee, zij spreken niet met mensen.

RS: Oh nou je hebt bijvoorbeeld wel de NGFG het Nederlands Vakgenootschap voor Functionarissen Gegevensbescherming en in september kwam daar bijvoorbeeld iemand van de autoriteit.

H2: Ja dat verslag hebben we wel vernomen ja. Dat ging dan over die datalekken en daar zeiden ze dat je redelijkerwijs moet kunnen uitsluiten dat. En dan begreep ik dat die persoon daar het woord redelijkerwijs schrapt. Je moet kunnen uitsluiten. Ja dat kunnen we nooit.

H1: Wat we dan doen is ook gewoon, we gaan gewoon uit van redelijkerwijs, want het is onredelijk om dat eruit te halen, want dan is het altijd foute boel. Je moet daar wel bij realiseren dat als je er verantwoording over kunt afleggen naar de rechter over hoe het gedaan is dan is het wat ons betreft oké.

RS: Ja en je hebt natuurlijk nu een soort tussenperiode want je hebt nu de meldplicht datalekken maar straks kan de Europese Verordening gehandhaafd worden, want hij is natuurlijk al van kracht. In hoeverre denken jullie dat je daarop voorbereid gaat zijn?

H1: Nou we hebben toevallig net een managementreview geschreven dat we een heel eind op weg zijn op basis van een overzicht dat is samengesteld met andere UMC's. Dus dat is wel zo'n erg handige Excel dan weten we nog precies wat we allemaal moeten doen, maar we verwachten dat we een heel eind op weg zijn. Weet je, we hebben bewerkersovereenkomsten, we hebben de Meldplicht Datalekken, we hebben alleen bijvoorbeeld zaken nog niet als die dataportabiliteit en onze transparantie is nog niet optimaal maar wel redelijk en dan hebben we ook natuurlijk nog het cliëntenrecht in de zorg.

RS: ja, dat je onder de keten zeg maar.

H1: Ja en toestemming hebben om informatie te verstrekken en om informatie te krijgen en dan moet het ook nog eens een keer gespecialiseerd zijn wat dus dat zijn ook dingen die op ons afkomen. En we hebben hier natuurlijk ook een data protection officer aangesteld, twee zelfs, met bevoegdheden als zodanig met een goede positie in de organisatie. Die AVG maak ik me niet eens zoveel zorgen meer over.

RS: Ja, want wat doen die data protection officers?

H1: Dat zijn wij.

RS: Oh, ik dacht al, daarom vroeg ik het ook want ik ken inderdaad een opleiding die heet Certified Data Protection Officer, maar ik dacht inderdaad dat dat hetzelfde was als functionaris gegevensbescherming, maar ik dacht even checken of dat wel zo is.

H1: Ja, dat is zo. Op een feestje klinkt het leuker als je zegt ik ben Data Protection Officer.

Nagesprek

RS: Nou hartstikke bedankt ik denk dat ik veel informatie heb gekregen dus ik kan weer verder met uitwerken.

5.9 Uitwerking interview zorginstelling I

RS: Eerst benieuwd eigenlijk hoe ben je op de positie van ICT-manager terechtgekomen?

Zorginstelling I: Dat komt omdat ik 25 of 30 jaar geleden als programmeur ergens begonnen ben en nooit wat anders ben gaan doen.

RS: Oké, dus al een behoorlijke tijd in dat vak.

Zorginstelling I: Een ouderwetse ICT'er zeg maar.

RS: Ja, en want ik zag dat je bezig was met een opleiding tot FG, hoe ben je daarbij terechtgekomen?

Zorginstelling I: Nou mede door de publicaties over die nieuwe WBP en de Wet Meldplicht Datalekken dat ik dacht 'ja daar moet iemand wat over weten binnen dit bedrijf' en toen ben ik daarmee begonnen. Ik ben inmiddels daar wel na de juridische procedures ben ik daar wel mee gestopt, dus ik maak die opleiding niet af.

RS: Oké, je bent ermee gestopt, wat was daar de reden van?

Zorginstelling I: Nou omdat ik dacht dat alleen het begin erg juridisch getint zou zijn, maar zij zeiden dat op een gegeven moment gaan we het over security hebben en maatregelen en weet ik veel wat en dan wordt het wat praktischer, dat zag ik niet, ik vond het niet heel praktisch worden en ik ben geen jurist. Dus ik vond het wel mooi geweest.

RS: Oké dus je hebt een beetje bijgespijkerd op het juridische vlak zeg maar.

Zorginstelling I: Ja en wat dat betreft ben ik nu wel goed op de hoogte wat betreft de Wet Meldplicht Datalekken.

RS: Ja, ja precies en want jullie hebben nog niet officieel een FG aangesteld, maar is er al wel iemand bezig met privacy en de bescherming van persoonsgegevens binnen de organisatie?

Zorginstelling I: Ik.

RS: Ja, en wat doe je dan zoal op dat gebied?

Zorginstelling I: Roepen dat het heel hard nodig is. Nee, het is absoluut niet onderkend hier dat we daar wat aan gaan moeten doen. Ik heb een nulmeting laten doen door een organisatie voor het hele bedrijf en die ligt nu bij de Raad van Bestuur en daar gebeurt niks mee op dit moment.

RS: Oké dus eigenlijk de Raad van Bestuur die heeft dit thema nog niet echt in beeld?

Zorginstelling I: Wel in beeld, maar ja ze acteren nog niet echt.

RS: Nee, nee en kan je verklaren waarom?

Zorginstelling I: Waarom weet ik niet, nee, ik weet niet waarom.

RS: Oké, misschien dat ze andere thema's eerst nog hebben liggen.

Zorginstelling I: Zou kunnen.

RS: Het is wel een redelijk belangrijk thema, zeker sinds de Wet Meldplicht Datalekken is ingevoerd. En je had het erover dat jullie in januari wel gaan beginnen met communiceren naar medewerkers. Is er verder al iets van beleid opgesteld?

Zorginstelling I: Nou omdat ik ook security officer ben, ben ik ook bezig met NEN 7510 en van daaruit moeten we NEN 7510 gecertificeerd worden volgend jaar. Eigenlijk ook als een onderligger op de Wet Datalekken. Het staat er niet keihard in als voorwaarde, maar het is feitelijk wel een voorwaarde vanuit de wet, dus vandaaruit dat ik ook dingen ga doen. Maar dat is meer mijn feestje dan het bedrijfsfeestje op dit moment.

RS: oké oké, dat is ook wel goed om te weten. Dat hoor je wel vaker hoor dat het door het bestuur nog niet echt wordt gedragen. En in grotere organisaties is het vaak iets makkelijker om het bestuur in dit soort dingen mee te krijgen. Want die NEN 7510 norm daar zitten natuurlijk behoorlijk wat voorwaarden aan, wat moet ik me voorstellen aan dingen die daarvoor gebeuren of dingen die op de planning staan?

Zorginstelling I: Er is eigenlijk al jarenlang een project geïdentificeerd om dat te doen en daar hebben we nu externe ondersteuning bij ingeroepen en we implementeren een managementtool daarvoor die de auditors en de maatregelen die daaruit komen echt monitort en op regelmatige basis ook bij stakeholders neerlegt. Dus het is eigenlijk een tool waarbij je die hele NEN-norm die stop je daarin en daar maak je dreigingsanalyses en impactanalyses en daar komen maatregelsets uit en die maatregelen koppel je weer terug aan stakeholders in het bedrijf. En die tool die monitort dan de plan-do-check-act cyclus van al die maatregelen bij al die stakeholders.

RS: oké dus dat wordt dan via die managementtool kun je een overzicht krijgen van wat wordt er nu op dit moment gedaan.

Zorginstelling I: Eigenlijk elke dag één druk op de knop en een real time audit van je hele normering van het hele bedrijf.

RS: En hebben jullie dan bijvoorbeeld ook al gekeken naar risico's voor jullie instelling?

Zorginstelling I: Ja, ja. Daar zit een risicoanalyse in en daar zit een dreigingsanalyse in.

RS: Ja, wat is daar het verschil tussen?

Zorginstelling I: Nou een dreiging is natuurlijk een brand is een dreiging maar dat hoeft nog geen heel groot risico te zijn, dus het is een beetje een woordspelletje.

RS: Nee, oké en ben je ook bekend met de 'ZEKER' campagne van de NVZ?

Zorginstelling I: Nee, wat is dat?

RS: Nou dat heeft te maken met de Alert Online weken die in oktober vaak gedaan worden in organisaties, in zorginstellingen en dit jaar hebben ze dat breder getrokken dus niet alleen naar ziekenhuizen maar ook naar andere zorginstellingen en dat is een campagne waar ze bijvoorbeeld medewerkers bewust willen maken van informatiebeveiliging.

Zorginstelling I: Oké

RS: Nou dat is dus die campagne ik vroeg me af of je daaraan mee hebt gedaan of niet.

Zorginstelling I: Nee, ken ik niet.

RS: Nee, dat is dus niet bij jou terechtgekomen die campagne. Nou misschien leuk om eens naar te kijken. Ook omdat er nog veel op touw gezet moet worden, biedt best grappige handvaten, dat is dan al bestaand materiaal zeg maar. Want ik weet niet of jullie een communicatieafdeling hebben?

Zorginstelling I: We gaan deze maand gaan we een bedrijf zoeken om ons met een Awarenesscampagne te helpen. Dus met wat jij nu zegt dat kan ik mooi meenemen. Ik hoor daar graag meer van.

RS: Ja, natuurlijk uit dit onderzoek komen ook inzichten en er zijn ook aardig wat mensen die hebben hier al redelijk beleid voor en die hebben al een beetje ontdekt van wat kun je nu beter wel doen en wat kun je nu beter niet doen.

Zorginstelling I: Dat is heel welkom die informatie

RS: Ja, dat kan ik me voorstellen en wat zijn voor jullie als instelling dan de grootste risico's?

Zorginstelling I: Nou wij zijn een VVT-instelling. Daar hebben we verzorgingstehuizen voor ouderen. Ja, ons grootste risico is dat er cliëntdossiers op straat komen te liggen. Ja aan de andere kant is dat ook weer niet zo'n heel groot risico. Als het gebeurt hebben we een ernstig probleem, maar de kans dat het gebeurt is niet zo heel groot. We moeten het wel zo doen.

RS: Waarom is die kans niet zo groot denk je?

Zorginstelling I: Nou ja dan moet je echt behalve de onwetendheid van de medewerkers hè zoals dat iemand een dossier uit z'n tas laat vallen onderweg of dat iemand hier iets laat liggen op tafel. Ja ik neem aan dat het hacken van deze instelling nou niet echt prioriteit is voor hackers, snap je. Dus in die zin het interesseert natuurlijk helemaal niemand dit. Het is alleen toeval en dommigheid waar die risico's ontstaan. Maar dat is wel iets waar een awarenesscampagne heel goed op gericht moet zijn, want mensen doen maar wat hoor.

RS: Jullie hebben op dit moment nog niet echt te maken gehad met datalekken of iets?

Zorginstelling I: Nee, nee.

RS: oké dat is misschien ook wel waarom het lastig is om het bij het bestuur onder de aandacht te brengen. Want hebben zij de gevolgen wel in kaart?

Zorginstelling I: Nou ze zijn zich er vaag wel van bewust, maar ze denken ook dat zal mijn tijd wel doen en het gebeurt toch niet. Dat zit er wel een beetje in, maar goed dat is voor een deel wel te begrijpen, maar het is niet oké. Je moet het gewoon goed regelen en technisch zit het allemaal best op orde hoor. Ik bedoel het is niet zo dat als je hier binnen loopt dat je alles zomaar te pakken krijgt, maar het is ook niet zo dat we een bank zijn, dus er zit altijd een financiële afweging aan in wat ik wel en niet doe. Ik heb bijvoorbeeld anderhalve maand geleden de screensaver op 4 minuten gezet en dat was al een schok hoor in het bedrijf.

RS: Oké dat werd dan niet echt gewaardeerd.

Zorginstelling I: Nee, daar is niemand blij mee. Dus ja als ik er dan zo'n campagne om heen zou hebben dan wordt dat voor mij ook makkelijker.

RS: Nu worden de maatregelen zeg maar al wel gedaan, maar de medewerkers die worden er nog niet echt in meegenomen.

Zorginstelling I: Nee, zeker de zorg niet. De overheid, zeg maar, de kantoormensen die worden er eerder in betrokken dan de zorgmedewerker op dit moment. Daar wordt toch nog wel van gedacht die willen het niet, die snappen het niet, die kunnen het niet.

RS: Want jullie hebben dan veel thuiszorg en veel verpleeghuizen denk ik?

Zorginstelling I: Nee, geen thuiszorg alleen verpleeghuizen.

RS: Oké dus iedereen zit wel op een locatie dat maakt natuurlijk wel dat ze op een manier te bereiken zijn.

Zorginstelling I: Ja, precies.

RS: Want hebben jullie daar al ideeën over, over hoe je de medewerkers gaat bereiken?

Zorginstelling I: Nee.

RS: Nee, oké en wordt de communicatieafdeling daar bij betrokken?

Zorginstelling I: Nou wat ik net zei. We gaan een bedrijf selecteren voor een awarenesscampagne en dat doe ik samen met communicatie. Ja in feite doe ik het samen met ze zeg ik maar ik ga dat stukje overdragen naar de afdeling communicatie. Hoe ze dat gaan doen laat ik graag over aan de mensen die daar verstand van hebben.

RS: ja, maar jij hebt natuurlijk wel de kennis.

Zorginstelling I: Ja, precies de inhoud is voor mij het belangrijkste.

RS: Ja, en waar denk je dan dat in de organisatie lastige punten zitten of zwakke punten om zoiets door te kunnen voeren?

Zorginstelling I: De zorgmedewerkers. Die zijn over het algemeen toch wat lager opgeleid en een aantal van hen ook slecht in taalgebruik. Er zijn een aantal medewerkers die slecht Nederlands spreken en die moeten het toch ook snappen.

RS: Ja precies en dat maakt het ook lastig natuurlijk om die vertaalslag te maken. Want hebben jullie nu iets van een reglement op het gebied van privacy of gedragscodes?

Zorginstelling I: Ligt allemaal ter goedkeuring.

RS: Oké dus dat ligt allemaal bij de Raad van Bestuur.

Zorginstelling I: Ja, directie en Raad van Bestuur.

RS: Want hoe groot is de Raad van Bestuur ongeveer?

Zorginstelling I: De Raad van Bestuur is één en de directie is vier.

RS: Oké maar er is niemand van de Raad van Bestuur die dit al in zijn portefeuille heeft?

Zorginstelling I: Ja, de Raad van Bestuur is er maar één dus die heeft niet eens een portefeuille. De Raad van Bestuur is één iemand. Maar de Raad van Toezicht zal dit ook op zijn agenda moeten hebben, alleen daar ligt het nog niet omdat het bestuur dat daar niet neerlegt. Maar misschien handig om te weten dat wij binnenkort een nieuwe bestuurder krijgen. Dus er zijn hier een aantal dingen die aan het veranderen zijn.

RS: Ja, ja.

Zorginstelling I: Dus dat is onvoldoende nu.

RS: Ja dus dat speelt dan ook mee natuurlijk zo'n reglement blijft dan lang liggen. Ik weet niet wanneer je het hebt opgesteld bijvoorbeeld?

Zorginstelling I: Dat durf ik niet te zeggen, nee.

RS: En zijn er in het algemeen regels?

Zorginstelling I: Ja zeker. Er is een soort ICT-reglement en er waren algemene gedragsregels, maar het is allemaal, het is er allemaal wel, maar of oud of niemand kent het of het is niet nog een keer goed afgestempeld of goed over gecommuniceerd. Het is gewoon aan alle kanten verstofd. Dus men moet gewoon weer helemaal opnieuw de molen door en worden opgefrist zowel op het gebied van privacy als op security als op informatieveiligheid, helemaal.

RS: Ja, want er zijn bijvoorbeeld geen mensen die erop toezien of het reglement goed wordt uitgevoerd?

Zorginstelling I: Nee.

RS: Dus, ja dan heb je misschien ook als medewerker snel zoiets van 'nou ja het zal er wel ergens zijn, maar ik doe mijn werk wel gewoon'.

Zorginstelling I: Ja, precies.

RS: En want er zijn dan nog geen incidenten geweest. Merk je bijvoorbeeld wel sinds de Meldplicht Datalekken is ingegaan dat er veranderingen zijn dat mensen er meer mee bezig zijn?

Zorginstelling I: Nee, ze weten helemaal niet eens dat die wet er is.

RS: Oké dat is wel interessant want in de media wordt er natuurlijk best veel aandacht besteed, sinds september, ik weet niet of het dan mij opvalt omdat ik met dit onderwerp bezig ben.

Zorginstelling I: Ik denk wel iets meer.

RS: Maar er zijn natuurlijk genoeg voorbeelden van datalekken.

Zorginstelling I: Maar die worden nog niet heel breed uitgetrokken.

RS: Wat bedoel je daarmee?

Zorginstelling I: Het valt jou op en het valt mij op, maar feitelijk is er nog niet heel veel bij dergelijke gebeurtenissen gedaan en de AP heeft ook nog niks gedaan. Die heeft nog niemand op zijn vingers getikt, dus wat dat betreft doen ze ook niet veel. Ja, er is één bestuurder op zijn vingers getikt, maar dat was niet zozeer

over privacy, dat was meer politiek. Daar werd men dan al zenuwachtig van. Maar niet echt op de privacy, meer gewoon in zijn algehele niet functioneren.

RS: Want hoe kijk je dan aan tegen de rol van de autoriteit?

Zorginstelling I: Nou die zou in mijn ogen toch wel als ze dit echt graag gedragen willen hebben ook in de bestuurskamer dan zouden ze toch wel een keer eentje op zijn vingers moeten tikken.

RS: Ja, omdat er eigenlijk nu niet genoeg angst is?

Zorginstelling I: Nou ja angst is een naar woord, maar goed hoeveel besturen hebben het privacyonderwerp in hun risicobegroting meegenomen? Nou heel weinig denk ik hoor, waarom die risico's die zijn er helemaal nog niet? Nou ja ze zijn er wel maar ze zijn niet zichtbaar.

RS: Nee, het kan natuurlijk ook zo zijn van we geven de bedrijven wel de kans om zich hieraan te conformeren want het kan natuurlijk ook averechts werken als zij met boetes komen.

Zorginstelling I: Ja, maar je hoeft niet meteen met acht ton te komen. Je kan ook een aanwijzing geven en die in de krant zetten of in ieder geval een keer publiceren: we hebben zoveel datalekken gezien en bij zoveel procent van deze datalekken hebben we ook een onderzoek gestart. Maar je hoort alleen maar ja er komt een nieuwe wet en het wordt zo streng en iedereen moet wat, maar ja goed als ze bij mij in de stad zeggen je mag niet meer rechtsaf en denk erom. En je doet er niks mee dan gaat iedereen gewoon rechtsaf. Dat is de menselijke natuur.

RS: Ja dat is natuurlijk ook waarom het nu is ingesteld dat fietsers wel rechtsaf mogen slaan bij stoplichten.

Zorginstelling I: Ja, ze doen het toch. Als je niet handhaaft, dan moet je ook geen wet instellen. Dat is eigenlijk mijn mening.

RS: Ja, ze hebben natuurlijk ook wel weinig capaciteit daar bij de autoriteit.

Zorginstelling I: Nou neem mensen aan zou ik zeggen.

RS: Ja, daar moet dan natuurlijk wel budget voor zijn ook bij de overheid.

Zorginstelling I: Ja, klopt. Maar ja als je boetes uitdeelt krijg je ook geld.

RS: Ja, dat is ook een goede inderdaad. Daar kunnen ze goed aan verdienen. En ken je bijvoorbeeld het Vakgenootschap voor Functionarissen Gegevensbescherming in Nederland?

Zorginstelling I: Nee.

RS: Ah oké dat is ook een vereniging die af en toe ronde tafel bijeenkomsten organiseert bijvoorbeeld voor FG's en laatst was daar ook iemand van de Autoriteit Persoonsgegevens bij aanwezig. Om onduidelijkheden en dergelijke over de wet te bespreken.

Zorginstelling I: Oké, hebben zij een website?

RS: Ja het heet Nederlands Vakgenootschap voor Functionarissen Gegevensbescherming. Ik ben daar toevallig bij geweest in september. Voor mij was dit iets minder interessant omdat het vooral op het juridische aspect inging, maar voor jullie wel interessant waarschijnlijk. Het ging vooral in op onduidelijkheden die in de wet staan en wat de Autoriteit Persoonsgegevens daar dan over te zeggen had, maar goed dat was even ter tip. Want je hebt natuurlijk die risico's nou die zijn nog niet heel goed in beeld bij het bestuur en misschien ook niet zo heel groot bij jullie. In hoeverre denk je dan dat communicatie zou kunnen bijdragen aan het inperken van die risico's?

Zorginstelling I: Nou omdat een heleboel mensen zich gewoon echt niet bewust zijn van het feit dat als je je kantoor uitloopt en je laat alles liggen dat je daarmee een privacyrisico loopt. Dat weten ze gewoon echt niet

en dat ze op de prikborden in de huiskamers gegevens over mensen als geboortedatum en weet ik veel wat allemaal het gaat gewoon ook niet echt ergens over maar het mag gewoon niet en nou ja van die dingen en je kunt wel zeggen hoe belangrijk is het? Ja het wordt pas belangrijk als iemand gaat zeuren of een klacht indient of iets dergelijks. Maar ik ben van mening dat wij ook als organisatie gewoon uiteindelijk de volwassenheid moeten hebben om aan die wet- en regelgeving te voldoen. Ja je kan wel zeggen van ik vind het niet nuttig, maar ja, dan moet je ook gewoon in je reclame-uitingen zeggen dat je dat allemaal niet wil en niet doet weet je. Wat dat betreft ben ik natuurlijk een ICT'er en het is een nul of een één.

RS: Ja, want ik kan me wel voorstellen dat er al wel redelijk wat privacybewustzijn is in de organisatie.

Zorginstelling I: Ja, maar men is zich echt niet bewust van de vergaande veranderingen die er nu zijn. Je mag niet appen, je mag geen foto's appen, je mag geen mailtjes met dossiers naar je familie sturen. En dan kunnen we met z'n allen wel vinden dat dat onzinregels zijn, ik vind dat prima, maar dan moet je dat voor dit bedrijf gewoon opstellen dat je dat onzin vindt en dat je je daarmee niet aan de wet houdt. Het mag, maar je moet het wel regelen.

RS: Ja, precies het zou niet het ideale scenario zijn natuurlijk.

Zorginstelling I: Ik zou het niet doen, maar ik vind dat je transparant moet zijn in wat je wel en niet doet. En als jij zegt ik vind het onzin ik doe niet mee met die flauwekul nou prima maar dan moet je dat wel gewoon vindbaar maken en ja het opvragen van dossiers en de procedures daarvoor het is natuurlijk een dramawet, want er zit erg veel werk aan te komen maar ja dan moet je zeggen dat doe ik niet.

RS: Het is natuurlijk wel belangrijk om er rekening mee te houden dat de Europese Verordening in 2018 van kracht wordt of in ieder geval handhaafbaar wordt.

Zorginstelling I: De vrijblijvendheid houdt op.

RS: Ja, ja precies, dus op een gegeven moment zul je toch acties hierin moeten ondernemen. Want worden er bijvoorbeeld op het gebied van communicatie andere campagnes gedaan op andere gebieden?

Zorginstelling I: Wat bedoel je?

RS: Ik bedoel bijvoorbeeld medewerkers informeren, hebben jullie bijvoorbeeld een intranet?

Zorginstelling I: Ja dat hebben we allemaal wel, we hebben ook gewoon een leerportaal en trainingen en dat soort zaken. Het is allemaal wel beschikbaar maar privacy en security staan gewoon niet op de agenda. Dus als het niet over zorg of over medische handelingen gaat dan is er gewoon geen interesse voor wat ik wel snap.

RS: Oké nou in ieder geval wel bijzonder dat ze het thema privacy nog niet op de agenda hebben. Ook niet in de zin van wat mag je wel en wat mag je niet. Dus daar zijn in ieder geval nog wel wat stappen te zetten. Ik denk dat er dan ook geen procedure is ingesteld voor als je een datalek zou ontdekken?

Zorginstelling I: Ben ik allemaal mee bezig om dat op poten te zetten nu. Protocol datalekken en het formeren van een commissie en dat soort dingen dat ben ik nu allemaal aan het doen.

RS: En ben jij dan de enige die zich hiermee bezighoudt met dit onderwerp?

Zorginstelling I: Nou dat is wel heel erg kort door de bocht. Laten we zeggen naar intensiviteit ben ik de enige ja. Maar dat neem ik allemaal mee in dat project NEN 7510, dus ik wil de komende twee kwartalen wil ik dat echt gaan uitrollen en daar gaat natuurlijk een heleboel in mee. Daar komt ook een datalekprotocol in en een commissie en vaststellen wie doet wat en wanneer en die awarenesscampagne waarin ik privacy gewoon meeneem, dus ja het gaat binnenkort wel allemaal gebeuren. Dat wel.

RS: Dus jij hebt daar eigenlijk een soort plan voor opgesteld nu en wat staat daar dan bijvoorbeeld in?

Zorginstelling I: Je bedoelt aan informatiebeveiliging enzo?

RS: Nou ja wat zijn bijvoorbeeld stappen te nemen in dat project?

Zorginstelling I: Ik ga het even voor je opzoeken. Ik weet ongeveer wel wat er moet gebeuren. Wat gaan we doen? Opleveren van het informatiebeveiligingsbeleid, de processen en documentatie het uitvoeren van de assessments en de analyses, de overdracht van kennis en kunde het implementeren van maatregelen en de controle op de naleving van de certificering en daar zit wel veel in en we hebben een nulmeting gedaan op privacy dus dat is net weer even een iets andere insteek en daar zit ook een enorme lijst aan activiteiten in, waarvan ik er wel een paar kan opnoemen. Verkrijgen van inzicht in de verwerkingen en het benoemen van eigenaren, beoordelen of er sprake is van een gezamenlijke verantwoordelijkheid, functieprofiel opstellen voor een FG, functieprofiel voor security officer, voldaan aan informatieplicht, nou ja een waslijst met activiteiten.

RS: Ja, want dat kwam dan uit die nulmeting van daar moeten stappen genomen worden.

Zorginstelling I: Ja, en dan meer op het gebied van privacy hè, want de NEN 7510 die is best wel gericht op de security en dit is dan weer echt voor de privacy.

RS: Heeft natuurlijk altijd wel met elkaar te maken die dingen en dan die nulmeting is gedaan en dan vanaf januari moet dit een beetje gaan rollen, want val jij dan onder de ICT-afdeling?

Zorginstelling I: Ik ben manager van de ICT-afdeling

RS: En heb je dan ook andere mensen die beschikbaar zijn die hier iets mee kunnen?

Zorginstelling I: Nee, nou ja dat laatste zou nog kunnen maar ze hebben geen tijd. Hier laat ik mij ondersteunen door een externe partij.

RS: Oké, want jij hebt er zelf dus wel voldoende tijd voor?

Zorginstelling I: Nou als je voldoende weghaalt dan klopt de zin.

RS: Ja, want hoeveel uur per week ben je dan ongeveer met het opzetten van dit project bezig?

Zorginstelling I: Dat is heel verschillend: de ene keer 10 minuten en de volgende keer dertig uur. Het is nog niet zo gestructureerd dat ik daar ook echt, kijk als dit nou gedaan is en we hebben dat managementsysteem voor de normering dan ga ik me ook weer wat strakker met privacy bezighouden, maar ja ik weet ook niet hoe de organisatie er over vier maanden uitziet dus dat maakt het niet makkelijker. Vandaar dat het toch nog een beetje mijn feestje is hier.

RS: Ja, want je hebt natuurlijk de Europese Verordening die eraan zit te komen in 2018 wordt die handhaafbaar in hoeverre denk je dat jullie daar op voorbereid gaan zijn?

Zorginstelling I: Nou 2018 daar heb ik wel een goed gevoel over. Die security krijg ik echt wel rond, dus die NEN 7510 en als je de NEN 7510 geregeld hebt dan ben je ook al wel een heel eind hoor ook met privacy die maatregelen zijn toch voornamelijk organisatorisch en schriftelijk. Nou dan komen we een heel eind, maar het moet wel gebeuren.

RS: Ja, zeker er moet wel animo zijn in de organisatie om hier iets mee te doen. Dat is natuurlijk belangrijk.

Zorginstelling I: En er moet een FG aangesteld worden.

RS: Nou die functie zou jij dan kunnen gaan vervullen of iemand anders.

Zorginstelling I: Nou wat mij betreft ook iemand anders, want anders wordt het ook erg chaotisch, dus voor mij hoeft het niet. Lijkt me nuttiger als ik diegene ondersteun.

RS: Ja je kunt ze natuurlijk ook extern inhuren.

Zorginstelling I: Ja, precies dat vind ik wel een heel aantrekkelijke optie. Dan zou ik wel gewoon aanspreekpunt kunnen zijn in de organisatie.

RS: Want er zijn dan ook nog geen vragen gekomen van medewerkers dat ze ergens mee zaten of dat ze iets zagen in het nieuws bijvoorbeeld?

Zorginstelling I: Heel incidenteel.

RS: En wat zijn dat dan bijvoorbeeld voor vragen?

Zorginstelling I: Nou bijvoorbeeld de vraag van een arts of die beeldmateriaal van patiënten op mag slaan en video-opnames van gesprekken en dat soort zaken dat soort vragen.

RS: Dus uiteindelijk er zijn nog wel mensen mee bezig.

Zorginstelling I: Nou hun vraag was dan vaak meer van een technische aard en dat ik zei van nou er zit ook een privacykant aan onderschat dat niet.

RS: Ja.

Zorginstelling I: Maar het valt heel erg mee. En je moet niet onderschatten hè de buitenwereld is er ook niet mee bezig hè. Maar als ik bijvoorbeeld een medewerker zou zeggen je mag helemaal dat dossier niet mailen nou de buitenwereld accepteert dat niet. Wij kunnen natuurlijk wel heel braaf alles tegen willen houden maar ja de zorg heeft te maken met familieleden en die hebben zoiets van 'ja weetje je zoekt het maar uit met je privacywetgeving. Je moet het me nu gewoon mailen nu'.

RS: Kan ik me wel iets bij voorstellen. Ook al zie ik zelf wel heel erg in organisaties dat ze er wel mee bezig zijn. Of dat ze bijvoorbeeld van een andere organisatie terugkrijgen van nou zorg maar dat je dat geregeld krijgt.

Zorginstelling I: Maar andersom ook hè. We moeten bijvoorbeeld allerlei gegevens aan de gemeente aanleveren omdat de gemeente van alles en nog wat betaalt maar dat kan niet veilig hè. De gemeente verdomd het om iets te regelen dat het wel veilig kan en als wij het niet leveren dan krijgen wij geen geld. Dat is pas krom. Dat zelfs de overheid zich weigert aan de regels te houden.

RS: Ja daar valt natuurlijk veel voor te zeggen over gemeentes. Als je kijkt naar het aantal datalekken in gemeentes, dat zijn er genoeg.

Zorginstelling I: Ja, dat zijn de grootste.

RS: Dus ja van alle kanten moet het eigenlijk nog meer aandacht krijgen dit thema. Ja, dat is natuurlijk ook de reden dat dit onderzoek is gestart. Ik denk dat ik genoeg informatie heb hierover. Ik denk duidelijk in januari gaat er hopelijk van alles gebeuren. En in januari wordt ook het resultaat van mijn onderzoek bekend. Streven is om eind januari terugkoppeling te geven.

Nagesprek

5.10 Uitwerking interview Zorginstelling J

Interview met 1 FG (J1) en 1 security officer (J2)

RS: Het is natuurlijk vrij nieuw de functie van functionaris gegevensbescherming. Hoe ben je op die positie terechtgekomen, vanuit welke achtergrond?

J1: Nou onze instelling heeft al heel lang een functionaris gegevensbescherming om te beginnen. Vanaf 2011 denk ik. Nou moet ik zeggen dat de invulling toen dat is denk ik niet meer helemaal te vergelijken met hoe het nu is. En hoe ben ik hier gekomen? Ja altijd affiniteit met recht gehad, ook recht gestudeerd maar niet

afgemaakt en het leek mij gewoon wel een uitdagende baan. En dat is begonnen met 4 uur in de week en nu zit ik op 8 uur in de week.

J2: En als het aan mij ligt wordt het fulltime.

J1: Ja, we zijn het er wel over eens dat bij zo'n grote organisatie als ons ziekenhuis, waar natuurlijk alleen maar eigenlijk persoonsgegevens worden verwerkt, er wel meer aandacht nodig is voor het hele privacyvraagstuk.

RS: En doe je daarnaast dan een functie als jurist?

J1: Nee, ik ben projectleider binnen bureau strategie en innovatie. Een mooie combinatie op zich.

RS: En jij bent dan security officer? (Kijkt naar J2)

J2: Ja, fulltime

RS: oké dus dat is wel een fulltime functie.

J2: Nou ja fulltime, 32 uur en ik werk er 40, zoiets.

J1: Maar officieel 32 uur. Wij zijn samen eigenlijk één FTE. En dan hebben we nog 8 uur een security manager binnen I&A, die echt dedicated voor security wordt ingezet.

RS: Waar staat dat voor I&A?

J2: De afdeling Informatisering en automatisering. Dus die echt intern binnen de afdeling zorgt dat de securityaspecten mee worden genomen, dus in de change in het problemmanagement. De security manager is ook voorzitter van het CERT ons Computer Emergency Response Team.

RS: Oké want vallen jullie dan ook onder die afdeling of?

J1: Ik niet. Ik ben de verlengde arm vanuit de Autoriteit Persoonsgegevens. Mijn functie staat ook in de Wet Bescherming Persoonsgegevens beschreven, waardoor ik als onafhankelijk intern toezichthouder m'n functie heb en daardoor aan het bestuur rapporteer als dat nodig is.

RS: Ja, dus daar ligt een directe lijn met het bestuur.

J1: Ik val dus niet onder een lijnmanager of iets.

RS: Maar dat staat dan dus eigenlijk rechtstreeks onder de Raad van Bestuur?

J2: Ja, en dat geldt voor mij ook. Ik val onder het bestuur en dat wisselt afhankelijk van hoe de bestuurders hun portefeuille verdelen. We hebben net weer een nieuwe bestuurder kwaliteit en veiligheid dus het kan zijn dat ik toch nog over ga naar deze bestuurder, maar dat is niet helemaal duidelijk. Ik zit nu nog bij F&C als stafadviseur en ik ga per 1 januari kom ik in de afdeling kwaliteit en veiligheid.

RS: Oké dus er is ook wel iemand in het bestuur aanwezig die dit onderwerp in zijn portefeuille heeft?

J2: Nou alle drie doen ze het, maar ze willen het er ook niet over eens zijn wie het uiteindelijk gaat doen. Ze vinden het alle drie interessant.

J1: Nou ik denk ook wel het boeiende met dit onderwerp. Het raakt feitelijk alle bedrijfsonderdelen van je organisatie. Of het nu gaat om patiëntgegevens, personeel, loongegevens of gewoon je bedrijfsinformatie, het raakt echt overal. Dus ik snap daarom ook wel de behoefte van de bestuurders om een gemeenschappelijke betrokkenheid te hebben zeg maar.

RS: En je hebt natuurlijk privacy en je hebt de bescherming van persoonsgegevens hoe staan die twee tot elkaar in verhouding?

J1: Nou privacy dat vind ik eigenlijk een wat naar woord, want ja wat is privacy? De bescherming van persoonsgegevens is eigenlijk dat je de persoonlijke levenssfeer respecteert en dat bedoelen we denk ik ook met privacy als we het er zo over hebben. Dus ja volgens mij bedoelen we hetzelfde of we het nu hebben over privacy of over Wet Bescherming Persoonsgegevens.

J2: En zeker als we straks naar de Europese Wetgeving gaan dan is dat helemaal helder, dat is gewoon één ding. En informatieveiligheid is een onderdeel van de norm dat is beschikbaarheid van informatie, integriteit van informatie en vertrouwelijkheid van informatie en ja wat is vertrouwelijkheid?

J1: Dus de kwalificatie van je informatie maakt hoe je ermee omgaat. Dat is eigenlijk het meest bepalend en ik merk dat dat iets is wat nog niet in de genen hier zit. We snappen allemaal dat onze parels zijn patiëntendata of onze persoonsdata, maar in combinatie of verwerkt in informatie is het nog wel eens lastiger om die parel te herkennen. Dan zit ie ver weg in de schelp en dan in één keer ontdekken ze 'goh het is misschien toch wel handig als we daar dezelfde eisen aan stellen als wanneer het gewoon heel duidelijk is' Dus daar zit nog denk ik als je het hebt over het ontwikkelingsniveau of het volwassenheidsniveau daar is nog wel wat winst te behalen.

J2: Ik heb volgens mij in 2011 mijn eerste beleid gegevensuitwisseling met classificatie van informatie geschreven. Dat was eigenlijk een soort van nieuw. Dat is net als dat 20 jaar terug Arbo nieuw was, is nu privacy en informatieveiligheid voor de zorgsector nieuw. Terwijl ze er wel altijd naar gehandeld hebben, alleen in begrippen en hoe je ermee omgaat dat is gewoon even een ander volwassenheidsniveau wat je gaat vragen.

RS: Ja, oké want er is toen al beleid opgesteld?

J2: Ja, ja, ja we hebben allerlei beleid.

J1: We hebben al heel veel beleid.

J2: We hebben privacybeleid, privacyreglement, dat was er eigenlijk als eerste, waarbij we al aangaven hoe we met dingen omgingen.
J1: En allerlei aanverwante zaken hè: camerabeleid, autorisatie, toegangsbeleid we hebben echt wel een hele waslijst daarover. Maar als je dan komt op jouw deel communicatie dan hebben we daar eigenlijk nog niet zoveel over.

J2: Twee brochures bij indiensttreding: één over de samenvatting van de huisregels informatieveiligheid, waarvan privacy een onderdeel is. En één algemeen over wat informatieveiligheid is. Medewerkers worden gescreend. Ze zijn verplicht om een VOG aan te vragen en we gaan ervanuit dat ze een geheimhoudingsplicht ondertekenen, dus daar zit in de entree, daar zit iets van brochures naar medewerkers. En ja we hebben brochures voor patiënten bijvoorbeeld, we zetten iets op de website over onze cookies, dus we doen wel wat, maar we doen zeker niet genoeg. Toevallig had ik gisteren een voorlichting bij radiologie. Ons beleid is dat er geen foto's worden gemaakt, alleen met toestemming van. Daar worstelen zij verschrikkelijk mee. Want iedere patiënt wil als die op tafel ligt in de buckykamer, wil een foto van zichzelf maken of de moeder wil dat van het kind en dat moet gelijk op Facebook en wij willen dat niet. Dus we willen dat niet om verschillende redenen: één er kan iemand op staan die daar geen toestemming voor heeft verleend, twee er kan bedrijfsinformatie op staan waarvan wij niet willen dat dat meegaat. Want die foto is niet meer alleen voor het fotoboek thuis voor later om voor het kind te zeggen van ja in die tijd lag je heel veel in het ziekenhuis kijk maar. Nee, dat gaat gelijk op internet dat moet met de hele familie worden gedeeld, dus je hebt een ander soort beleving daarbij en dat maakt het voor medewerkers soms lastig om te communiceren naar die patiënt van dat mag niet. En dan zegt die patiënt van: 'Ja wat een onzin waarom mag dat dan niet dat is toch mijn eigen foto? En als je het dan uitlegt dan snappen ze het ook wel, maar eigenlijk is er heel veel weerstand tegen, dus toen zei één van de medewerkers van 'kunnen we geen posters ophangen met: foto's maken dat doen wij?' Ja, dat vonden wij een

hele leuke, dus die heb ik ook meteen opgeschreven dus daar gaan we denk ik ook wel over nadenken om daar medewerkers van radiologie bij te helpen, maar misschien ook wel op de spoedeisende hulp.

RS: Ja, want als er beleid opgesteld wordt, wordt dat dan door jullie opgesteld of door de Raad van Bestuur?

J2: Nee, de Raad van Bestuur keurt alleen maar goed.

J1: Nou jij bent de grootmaker zeg maar van beleid en daar waar het kan maak ik ook beleid maar dat druist natuurlijk feitelijk in tegen mijn functie.

J2: Zij helpt me er alleen maar mee.

J1: Maar ja weet je als je maar één FTE hebt die dat moet faciliteren, ja dan ga je roeien met de riemen die je hebt. Dat is eigenlijk het verhaal.

J2: Maar we hebben als ziekenhuis een heel goed netwerk en we maken dankbaar gebruik van elkaars stukken. Nou was ik wel één van de eerste die stukken schreef zeg maar binnen het vakgebied. Maar daar zijn al heel veel varianten op gekomen en er zijn ook mensen die weer iets doen wat ik nog niet had gedaan, dus ja daar doen we het betere jatwerk. Want we zijn allemaal vaak projectmedewerker of maar een halve FTE, dus het is nogal een zwaar onderbemande functie voor het werk dat er ligt.

RS: Ja, want hoe kijkt de Raad van Bestuur dan tegen dit thema aan?

J2: Nou ze nemen het wel serieus nu.

J1: Je merkt dat het laatste half jaar er wel een verandering is opgetreden ook sinds de komst van de Wet Meldplicht Datalekken dat ze toch wel iets meer doordrongen zijn van 'ja dit is toch wel serious business waar we mee te dealen hebben'. En we zien daar ook wel beweging in komen en natuurlijk gaat dat allemaal niet van vandaag op morgen we zien in ieder geval dat daar een positieve tendens aan het ontwikkelen is.

J2: Ze zijn bereid om ons te gaan ontzorgen met inzet van externen. Dat kost altijd weer werk, maar dat maakt niet uit. Er komt wel wat.

RS: Dus zij zijn er wel mee bezig om het aandacht te geven?

J2: Ja, want ik heb nu ook een juridisch medewerkster al sinds driekwartjaar die nu afstudeert voor privacy onder andere en die doet al mijn bewerkersovereenkomsten, dat is gewoon een gigaklus en dat krijg je er echt niet bij in je uren. Dan hadden wij nu ook geen gesprek gehad.

J1: Nee, maar het feit dat dat ook kan zie je ook wel dat het bestuur zich ook wel van doordrongen is van 'hee er moet daar wat gebeuren we zullen dat anders moeten gaan organiseren die vraagstukken die er al liggen en die op ons afkomen'

RS: Want zou je dan zeggen dat privacy een hoge prioriteit heeft in jullie organisatie of een lage?

J2: Nee, wel een hoge.

J1: Het is hoger dan dat het was.

J2: Het staat in het risicoprofiel van de organisatie, daarin is het ook benoemd. Ze hebben het vorige week maandag met het MT besproken en toen werd er ook nadrukkelijk gezegd van is het wel nadrukkelijk genoeg beschreven, moeten we het niet wat hoger nog op de prioritering zetten? Cybercrime staat er ook op. Dus het is de combinatie van de dreiging en wat je verplicht bent om te doen en die combinatie maakt dat men het dus hoog op de agenda heeft staan.

RS: Ja want wordt het dan bijvoorbeeld ook meegenomen in overleggen bij ander personeel? Dus niet alleen in het management, maar ook in de rest van de organisatie?

J1: Ja, bijvoorbeeld vorig jaar hadden alle serviceassistenten een training. En die hebben we ook allemaal meegenomen in wat is nu privacy en dat is behoorlijk platgeslagen, maar dat zijn wel de mensen die de lakens bijvullen en het eten delen, maar die krijgen wel vragen van bezoek, van de patiënt in bed, maken we een fotootje, doen we dit, het is natuurlijk een hele kwetsbare groep in de organisatie die geneigd zijn veel te vertellen uit goedbedoeldheid, maar dat kan natuurlijk niet. Dus daar investeren we in. Alle nieuwe medewerkers, doet J2, is er altijd een introductiedag op de eerste maandag van de maand, die worden allemaal geïnformeerd over wat doen we, maar het is niet voldoende, want je merkt dat het ook herhalen is, praktische voorbeelden blijven benoemen en het is een taai onderwerp, het is absoluut niet sexy. Teammanagers die vinden het soms maar onzin, je hebt ook managers die nog steeds zeggen van 'hè nou moet dat allemaal en wat krampachtig'. Nou onze uitdaging is om niet krampachtig te zijn, maar te kijken naar hoe kunnen we wettelijke verplichtingen integreren in lopende processen zonder dat de professionals, de zorgprofessionals daar heel veel last van hebben en dat is natuurlijk de grootste uitdaging.

J2: Ik doe van de week nu vier werkoverleggen. Drie bij radiologie, want die club is zo groot dan hebben ze drie kansen zeg maar om te gaan en bij revalidatie morgen en dan is de insteek vanuit de discipline ook al verschillend, want bij R&N hebben ze het over de foto's maken, bij revalidatie hebben ze het over de gegevensuitwisseling. Maar zo zitten er een aantal dingen die dan inherent zijn aan dat proces dan nodigen ze je uit en dan doen we een stukje voorlichting en onderricht en dat is een halen brengen verhaal. Want ik vertel wat over wat ons beleid is, hoe het zou moeten, waar aandacht voor zou moeten zijn en je haalt ook, want je hoort ook incidenten, je hoort ook waar ze tegen aan lopen en dat kun je weer meenemen in je beleid, dus daar zijn die werkoverleggen sowieso goed voor. Als ergens een incident op een afdeling is dan is één van de sanctiemaatregelen, is altijd dat er een werkoverleg komt en dat de betrokken medewerkers daarbij aanwezig zijn. En dat bedoel ik niet heel zwaar.

J1: Het is niet als sanctie, maar als leren van hè .

J2: Kijk wat je doet is eigenlijk zo van laten we nou met zijn allen leren van wat we fout hebben gedaan en laten we er vooral extra weer attent op zijn, want het gebeurt heel snel, heel makkelijk, onbedoeld ook. En dat is waar mensen werken, worden fouten gemaakt en daar kun je met elkaar van leren, maar het is wel altijd een aanleiding om te zeggen van 'goh nou laten we dat dan even doen'. Plan mij in voor het eerstvolgende werkoverleg en meestal doen ze dat dan ook braaf.

RS: Want dat verzoek komt dan wel vanuit hen om langs te komen?

J2: Ja, ja, ja en ik let ook wel op of ik afdelingen niet heb gehad, dus ik heb nu even weer geturfd en dan zie ik dat vanuit de FB (facilitair bedrijf) niets komt. Dus dan ga ik de manager FB weer even aanschrijven en dan zeg ik van 'wat mij opvalt is dat jullie op geen enkele vorm blijkbaar iets gedaan hebben aan informatiebeveiliging, kun je mij het tegendeel bewijzen? Dat ik iets heb gemist misschien dat jullie dat allemaal zelf doen aan de hand van onze mooie pagina informatieveiligheid en privacy. Dat zou zomaar kunnen maar ik weet het niet. Dus kun je me het dan even vertellen?'

RS: Oké dus daar wordt dan wel op toegezien?

J2: Ja, dat hoort in onze plan-do-act-check cyclus te zitten dat we af en toe controle doen, maar ja dat is het eerste wat erbij inschiet. Maar dit soort dingen doe ik tegen het einde van het jaar voor het overzicht naar de Raad van Bestuur van wat is er nou gebeurd dan wil ik wel altijd even checken en dan zijn er wel dingen die opvallen. Bijvoorbeeld goh die afdelingen komen wel regelmatig langs en daar gebeurt ook van alles, maar daar gebeurt niks.

RS: En er is dus een pagina informatiebeveiliging op het intranet is dat?

J2: Ja, ja we hebben een pagina.

RS: En is er ook al gecommuniceerd naar medewerkers toe dat die pagina er is?

J2: Ja.

RS: En op wat voor manier is dat gegaan?

J2: Via de teammanagers.

J1: En we hebben meegedaan met de Alert Online campagne.

RS: Dat was ook één van mijn vragen inderdaad.

J1: Hebben we ook met een kraampje bij het restaurant gestaan met folders en informatie en noem maar op en daar hebben we ook iedereen geattendeerd op de community en ga daar eens naar toe en daar zijn leuke vragen uit gekomen en foldertjes meegegeven, dus zo proberen we het steeds te verbreden eigenlijk.

RS: Want dat was dan een soort informatiemarkt of een kraampje van jullie?

J1: Een kraampje van ons en dat hadden we gewoon strategisch neergezet dat als je ging eten dan kon je niet om ons heen eigenlijk. En dan was het natuurlijk nog wel aan degene om wel of niet aan te haken bij dat kraampje. Maar kijk wij kennen veel mensen in het ziekenhuis dus je kan ook met een lolletje wat makkelijker van 'hee heb je dit al gezien of hoe doen jullie dit?' Je kan wat ontspannen iemand betrekken bij het onderwerp zonder dat je met een opgeheven vinger gaat staan.

J2: Kijk dit was ons standje. Dit is onze bestuurder en dit is de security manager van I&A.

RS: En dan staat er dus ook weer een berichtje van op intranet.

J2: En we hebben ook in die week heel veel blogs geschreven, bijna dagelijks. Hebben we blogs geschreven aan de hand van het thema van de NVZ, de week van de privacy heb ik mensen op geattendeerd dat dat op televisie kwam.

RS: En dit komt dan op een soort startpagina van het intranet?

J2: Ja dat is hier is dan de nieuwspagina. Hier hebben we ook gestaan zeg maar (wijst op bovenstuk websitehomepagina) dus nu komen er alweer verschillende andere artikelen en daar zag je ons ook langskomen.

J1: En je hebt ook een tijdlijn. Dan popt het daar ook op en dan kan je ook reacties doen en dingen.

RS: Ja, dan krijgt het onderwerp natuurlijk ook weer aandacht. En hebben jullie ook meegedaan met die test?

J2: Zeker zorg die? Drie mensen. Met een goede uitslag hoor. Het is grappig dat je maar drie man nodig hebt om het beeld te bevestigen dat je zelf hebt. Klinkt niet valide, maar het was wel zo. Het verbaasde mij echt. Er kwam uit dat wij de eerste twee punten niet goed hadden en dat klopt ook. Weetje het beleid is bekend dat is er allemaal wel.

J1: We hebben ook e-learling, zit ik even net te denken, die iedereen volgt.

J2: Ja, die zit nu in het LMS en die moeten ze volgen daar krijgen ze ook een punt voor, ook de leden van de medische staf. Medische staf wordt bij ons ook apart voorgelicht doe ik ook één keer per jaar minimaal. Ik word bij het dagelijks bestuur van de medische staf één keer per jaar uitgenodigd voor de vergadering. Cliëntenraad die zijn vernieuwd. Dus ik bedacht net dat ik de nieuwe voorzitter moet aanschrijven dat we daar weer een keertje langsgaan. Ondernemingsraad staat weer op m'n agenda, want die verspreiden ook informatie, dus

daar moet ik ook weer iets van voorlichting en onderricht gaan doen, die mailen ook naar iedereen, dus ik dacht oja dat is weer een dingetje. Dus zo proberen we wel die communicatie goed op gang te houden.

RS: Ja, dus dat alle groepen in de organisatie in ieder geval bezocht worden.

J2: Ja en het is wel grappig want ik onderteken met die 'wees alert, wees bewust, wees zorgvuldig'. En nu hadden we het wachtwoordbeleid, hadden we een aanpassing gedaan, dat we om de 150 dagen ons wachtwoord moeten wijzigen en dan hadden ze een brief gemaakt met mijn naam eronder, maar dat is een script wat dan naar 600 medewerkers tegelijk gaat en toen hadden ze dat logo er niet bijgezet. En we hebben een virus gehad en toen heb ik een mail uitgestuurd naar alle gebruikers, erop gewezen dat we het tijdelijk zouden blokkeren en iedereen voorzichtig aangegeven: 'klik niet op de phishingmail', de phishingmailactie hebben we trouwens niet aan meegedaan. Ik was op vakantie en ik was te laat met aanmelden. Maar goed nu kreeg men dus die mail met mijn naam eronder, maar zonder dat logo en dat is aanleiding geweest voor vier mensen om mij te bellen en te vragen is dit geen phishingmail want er staat een link en jij communiceert altijd met dat logo en nu staat dat er niet bij, is dit wel van jou? En toen dacht ik nou dit is winst, dat betekent dus mensen letten goed op, mensen zeggen van klopt dit wel? Ik moet nu op een linkje klikken. Dus dat betekent wel dat je die alertheid bij de gewone gebruiker dat je die wel bereikt hebt. En als ik me soms voorstel aan een gewone verpleegkundige die ik zelf niet ken of die ik ooit bij een introductie heb gezien en dan zegt ze van ja maar ik ken je wel want ik krijg wel eens mail van jou en heb je naam wel eens gehoord of ik zie het wel eens en dan denk ik van nou ze relateert wel aan jou als persoon en de boodschap die hebben ze dan meestal toch ook wel meegekregen.

RS: Ja.

J2: Nou dan heb je toch zoiets…

J1: Maar daar werk je ook al heel wat jaartjes aan.

J2: Uhm, vanaf 2010 dus, ja 6 jaar.

RS: Dus al best lang bezig. En bij zo'n voorlichting bijvoorbeeld wat voor informatie wordt er dan gegeven aan medewerkers?

J2: Nou ik laat een Youtubefilmpje zien van hoe makkelijk je al je informatie op internet en hoe je daarbij kan komen en dan vertel ik gewoon even de grote lijnen van wat kun jij hier zelf doen en wat doen wij, wat proberen wij ook om jou technisch te ondersteunen om het makkelijk te maken, dus bijvoorbeeld dit (laat zien hoe je in en uitlogt door enkel je pasje te scannen) dat hadden we toen nog niet en nu hebben we dat wel en dat betekent dat ik ook verwacht dat iedereen heel snel in en uitlogt.

J1: Ja en dat is nog wel een puntje.

J2: En dat is nog steeds een puntje. Vanochtend had hier op de afdeling een externe die werd ingehuurd haar scherm openstaan en toen had iemand haar muis omgezet van links naar rechts en iedereen eromheen wist het en zat te wachten tot ze zou exploderen omdat ze niet meer snapte wat er gebeurde. 'Ja' zei een collega 'je weet het hè, J2 zit daar en dat mag niet hè'.

J1: Beetje hardleers.

RS: Hier is het bij de afdeling misschien ook iets logischer dat ze er iets mee doen.

J2: Nou nee hoor hier bij de afdeling was het in het begin echt een uitdaging.

J1: Wat ik wel mooi vond ik was vanochtend bij de fysiotherapie, want ik zag in het screen de foto van het team en toen vroeg de ene fysio aan de ander ja waarom heb je die foto van ons daar zo staan? Ja zegt die andere fysio maar anders zie je de persoonsgegevens. Dus hij logt dan niet in en uit omdat ze zoveel continu van

patiënt naar patiënt gaan, maar hij zegt ik heb het zo ingesteld dat als ik er dan niet in ben dat er een screen komt van een foto van ons fysioteam en dan zie je geen persoonsgegevens. Nou toen dacht ik of het ideaal is is een tweede, maar het gaat om de gedachte en daar gaat het om. Dat is wat je natuurlijk wil dat zij erover gaan praten. Je moet ergens beginnen.

RS: Ja want wat zijn dan voor jullie als instelling mogelijke gevolgen van bijvoorbeeld een datalek of een issue in de beveiliging?

J2: Wat bedoel je nu precies? Want een datalek hebben we, dat komt gewoon voor.

RS: Als in de risico's voor de instelling.

J1: Hoe we dat dan communiceren bedoel je?

RS: Nee, bijvoorbeeld wat zijn punten voor de Raad van Bestuur die van belang zijn om te voorkomen dat we datalekken krijgen?

J1: Nou ze willen sowieso geen datalek, omdat je vertrouwen wilt en je imago maar je wilt ook gewoon dat er geen dingen op straat komen te liggen waarvoor het niet bedoeld is, dus het bestuur die wil gewoon überhaupt niet dat er datalekken plaatsvinden. Dat willen wij ook niet.

RS: Nee al is het niet te voorkomen eigenlijk.

J1: Nee, zeker niet als het van buitenaf is. Kijk van binnenuit kan je natuurlijk heel veel doen want dan is het veel gedrag. Dan heb je het toch over voorlichting, mensen bewust maken.

J2: Ja, met die foto hebben we het gewoon echt niet gezien. Dat was ook iets de proefdruk op het beeldscherm was anders dan de druk op papier, waardoor je op de papierenversie met een vergrootglas de patiëntgegevens kon lezen, terwijl ze het gecontroleerd hadden op het scherm en ja dan kun je zeggen van wat slecht, maar dat heeft echt met nog weer scherper bewustzijn te maken van dat het er daar dan toch weer anders uitziet dan dat het hier op papier staat en dat iedereen tegenwoordig een vergrootglas op zijn telefoon heeft zitten en dat je dat dan ook kunt zien. Mensen met goede ogen kunnen dat ook zien.

J1: Ik vind wel dat met die nieuwe privacywetgeving op een bepaalde manier we ook wel lijken door te slaan.

J2: Ja dat vind ik ook.

J1: Maar goed identiteitsfraude is wel iets dat één van de grootste risico's is van een datalek wat je moet communiceren, want dat vond ik in het begin heel lastig van wat vertel je nou aan een patiënt waarvan de data gelekt is wat het risico is? Wat is nou het risico? Dat weet je niet altijd. En soms weet je wel waar de informatie terecht is gekomen bij een verkeerde persoon of er is per ongeluk een lijstje naar een patiënt opgestuurd en die patiënt heeft het dan weer netjes teruggegeven, maar daar stonden dan vijf andere patiënten op met hun naam en geboortedatum en dat ze bij een bepaald specialisme zijn gekomen, maar goed we hebben al die patiënten netjes geïnformeerd. Dat is de communicatie daarover dat je transparant bent dat dat is gebeurd, het is echt crisiscommunicatie hè.

RS: Ja, want is er dan een procedure ingericht voor de meldplicht datalekken dat mensen kunnen melden en dergelijke? En hoe is dat gecommuniceerd?

J2: Ja op de gebruikelijke manier.

J1: Ja, via het intranet, maar ook in de nieuwsbrief van de kliniek bijvoorbeeld. Vastgesteld dat het een bestuurlijk besluit is en we zitten nu eigenlijk nog in de afronding van de nieuwe versie.

J2: Ja, want we hadden er al één voor de wet.

J1: Ja, vooruit geanticipeerd hadden we dus ja als dat dan bekrachtigd is dan communiceer je er weer over. En ja het management die moet dan ook zijn teamleden daar weer over informeren, dus het is dan vanuit de lijn dat naar beneden moet worden gecommuniceerd nou ja en jij doet heel veel voorlichting en introductie en daar is het ook gewoon een item.

J2: Ja iedere introductie zeg ik 'Meldplicht Datalekken' en als er een datalek is willen we worden gebeld, niet alleen gevimd maar ook gebeld want dan moeten we binnen een bepaalde tijd handelen en nou ja dat gebeurt ook.

J1: Denken we.

RS: Dus ze kunnen intern melden via dat VIM-systeem en ze kunnen bellen.

J2: Nou ja kijk dan weten we nog niet hoe dat gaat lopen hoor. We hebben eigenlijk drie soorten meldingen. Eén gaat via de helpdesk, dat is wat er bij de helpdesk binnenkomt. Hè zoals we hebben een storing of informatie is niet beschikbaar, dus dat is ook een vorm van incident. Als de vertrouwelijkheid wordt geschonden dus er is de verkeerde mail naar buiten gegaan, dan horen we het ook via die weg dus dat zijn meldingen die bij de helpdesk binnenkomen. Dan heb je de meldingen die of bij J1 of bij mij binnenkomen en dan heb je nog de meldingen die voortkomen uit de VIM-meldingen. Dus dan ziet een VIM-commissie dat het gaat om informatieveiligheid of privacy en dan komt het ook bij ons.

J1: En dan heb je nog de bron de klachten van de patiënt, dus het kan zijn dat de patiënt een klacht heeft ingediend bij het patiëntenservicebureau en dat daardoor een incident boven tafel komt.

J2: Dat zijn eigenlijk de stromen die je probeert bij elkaar te brengen. En ik hoop daar volgend jaar nog een wat betere tool voor te hebben dat dat allemaal wat makkelijker met elkaar verbonden wordt, maar dat loopt er een beetje achteraan. We beginnen met excellijstjes en dan wordt het beter.

RS: En de medewerkers die hebben het dan via hun managers en medische staf ook op dezelfde manier? En hebben jullie ook iets van folders of iets dergelijks gemaakt?

J2: Brochures is nog wel een dingetje.

J1: Brochures dat behoeft gewoon aandacht, daar moeten we echt nog wel een slag in maken.

J2: Ja, daar hebben we het ook met de manager communicatie over gehad. En dat zit hem ook vooral in dat hele toestemmingsverhaal van de patiënt dat zullen we toch steeds beter en goed moeten communiceren. Dus zowel naar onze medewerkers als naar de patiënten. Ik had laatst een login van een patiënt en die was echt verbaasd dat hij ineens een nieuwe bezoeker login zag staan. En toen zei die: huh is dat een onderzoeker? En toen zei ik: Ja heeft je hoofdbehandelaar dat niet met je besproken want wij zijn een STZ-ziekenhuis en dan weet je toch dan doen we onderzoek.

J1: Staat ook op de website.

J2: Ja, maar daar heb ik eigenlijk nooit bij stil gestaan en dat is ook zo ik denk dat het ook zo werkt. En dat betekent dat er toch nog ondanks dat er een informed consent ligt dat je toch nog iedere keer weer extra moet zeggen.

J1: En dat dwingt de AVG natuurlijk ook af.

RS: Ja, want overleggen jullie dan met communicatie? Is dat een afdeling of?

J2: Ja, we hebben een vaste medewerkster bij communicatie.

RS: Oké en dat is dan de contactpersoon voor als jullie iets willen?

J2: Nou als er een incident is of alert online en afhankelijk van wie er dienst heeft, want zij draaien ook diensten.

J1: Ja maar de brochures die lopen feitelijk anders, want als er bijvoorbeeld een brochure gemaakt moet worden dan maak ik die brochure en communicatie kijkt alleen van klopt het in de juiste lay-out en that's it, dus dat moet je wel zelf doen. Communicatie maakt geen folders. Dat zullen wij echt zelf moeten doen.

J2: Ja en dat maakt het dus dat ik soms denk had ik maar een afdeling communicatie die dat wel deed.

RS: Ja, want wat doet communicatie dan bijvoorbeeld wel? Want als er iets van beleid opgesteld wordt, is er dan bijvoorbeeld ook een hoofdstuk communicatie?

J2: Ja, ik heb een communicatieplan dat schrijf ik ieder jaar opnieuw dat hoort in het kader van de NEN-7510 gaat ook naar de bestuurder en het ligt vast dat we bepaalde acties doen zoals alert online en daar wil ik ook budget voor, een minisymposium, brochures, e-learning dat kost allemaal geld, dus dan moet je dat begroten, dus ik laat communicatie dan een plan maken. Maar wat je ziet is dat communicatie ook een soort van in de waan van de dag leeft en dat maakt: de basis beheersdingen die hebben daar gewoon nooit een prioritering. En ik denk wel eens hoe kan ik dan ontzorgd worden door een afdeling communicatie? Is dat er iemand heel actief zegt van 'Oja, dit is jouw communicatieplan jij zou toch bloggen? Zal ik even een opzetje maken wat is je onderwerp?'

J1: Ja, want kijk eens hoe gebruiksonvriendelijk onze website is voor de patiënt, het is een gedrocht. En eigenlijk zou je willen dat de afdeling communicatie zegt van goh ik zie zoveel informatie ik stel voor om dat even in een andere vorm te gieten zodat het toegankelijker wordt en beter benaderbaar. Wij zijn geen communicatieadviseurs, dus wat doe je? Ik gooi het er allemaal op en dan denk ik ja dan staat het er maar, maar het klopt natuurlijk niet.

J2: Ja en ik ben gewend om beleidsstukken te schrijven, maar dat betekent niet dat dat een communicatiestuk is.

J1: Maar ook de aanvraagformulieren het is het allemaal net niet.

J2: Dus dat is wel een worsteling kan ik je vertellen.

J1: Daar hebben we gewoon hulp bij nodig.

J2: En het punt is dat heb ik nu ook tegen de nieuwe manager communicatie gezegd: ik wil daar gewoon letterlijk in ontzorgd worden. Ik wil gewoon een communicatiemedewerker die uit zichzelf bedenkt hé het is november daar zit de week van de privacy in want dat heeft ze gegoogled en dat heeft ze gezien en gaan we daar wat mee doen?

J1: Nou liever nog: ik heb een idee wat we zouden kunnen doen. Want nu lopen wij folders te maken, eigenlijk lopen wij alles zelf te doen.

RS: Maar dat is wel een goed punt natuurlijk, want daarmee zie je ook inderdaad wat veel bedrijven wel hebben is privacybeleid, gedragscodes en regels en dergelijke.

J1: Ja, dat gaat niemand lezen.

J2: De introductie, dat ben ik echt van mening, daar moet je het doen. Daar zit de kracht. Dan moet je een geheimhouding tekenen en daar staat in je bent akkoord met en dan tekenen ze dus voor iets en dan lezen ze het. En dat merk ik ook als ik die voorlichting geef dat mensen dan vragen stellen, helemaal goed dan heb je het gelezen. Maar dat is eigenlijk te weinig, want daarna gaat men mee in de waan van de dag en dan is men

aan het werk en dan gebeurt het dus niet meer. Als je er in de werkoverleggen geen aandacht aan besteed wordt, wordt het niet gelezen, als het niet opgenomen wordt in de notulen, als je er niet een PowerPoint achteraan stuurt en zegt van er zitten twee leuke filmpjes in dat moet je kijken stuur hem door vooral ook met je kinderen thuis bekijken zo breng ik dat dan en dan hoop ik dat ze het ook zien en kijken. Maar dat zijn dingen die ik bedenk en die ik doe.

RS: Maar er worden bijvoorbeeld geen bewustwordingscampagnes of iets dergelijks opgezet?

J2: Nou niet op die manier, als wij het niet initiëren niet.

RS: Want hoe ligt de communicatie-afdeling hier? Hoe ligt die afdeling binnen de organisatie?

J2: Valt ook onder de Raad van Bestuur.

RS: Maar zit de manager communicatie bijvoorbeeld in de Raad van Bestuur?

J2: Nee, die zit niet in het MT. Vroeger wel, nu niet meer. Het MT is heel klein geworden, maar de manager communicatie zit wel in het informeel overleg.

J1: Ja, maar wie zit daar niet bij.

RS: En als je dan bijvoorbeeld kijkt naar de AVG, want we hebben natuurlijk nu een soort tussenperiode. De AVG is al van kracht, maar wordt nog niet gehandhaafd. In hoeverre denken jullie dat jullie tegen die tijd voorbereid gaan zijn?

J1: Nou ja we hebben nog een jaar hè of nou ja anderhalf en we zijn best een eind op weg.

J2: We zijn best een eind op weg. We hebben een nulmeting laten doen door Deloitte voor ons privacybeleid, daar kwamen natuurlijk ook communicatiedingen uit. Eén van hun voorstellen is om privacycontactpersonen aan te stellen op de afdelingen en om met dat netwerk te gaan werken om die communicatie te verwerken. Nou dat kennen we ook al van de ERGO-users van de Key-users en weet ik het wat. Dus dat is een mooi netwerk waarvan je zegt van nou soms mensen die een incident mee hebben gemaakt, die kun je een soort ambassadeur maken voor het onderwerp en die zijn dan in een keer heel fanatiek en die mailen je ook van alles toe dus daar en ik denk dat als we dat officieel maken en we doen 1 of 2 keer per jaar een bijeenkomst met die privacy officers dan hebben we natuurlijk al een goede mogelijkheid om dat te communiceren denken wij met Deloitte gaan we dat dan nu doen, maar dat is nog zonder communicatie. Dan hebben we de communicatie die eigenlijk ook moet met onze derden waarmee wij gegevens uitwisselen: de bewerkersovereenkomsten maar ook alle kleintjes wat gewoon op een politie gebeurt daar moeten we ook nog iets mee. Dus ik dacht van ja hoe gaan we al die stakeholders nog een keer communiceren? Daar loop ik wel al een poosje over na te denken maar ik weet nog niet zo goed hoe.

RS: En kun je dan met dat soort vragen wel bij de afdeling communicatie terecht?

J2: Ja, ik kan het stellen maar dat wil niet zeggen dat ik een antwoord krijg. Dat is wel echt zo.

J1: Ik denk dat wij wel een beetje worstelen met hoe op dit moment de afdeling communicatie is ingericht of dat nog tegemoetkomt aan de eisen die er heden ten dage aan communicatie worden gesteld. In alle vormen die tegenwoordig ook mogelijk zijn en de snelheid van nieuws en van hoe breng je nou iets dat het toch blijft hangen? Want dat is natuurlijk waar het om gaat. Kijk onze intranetpagina is leuk maar als je één dag niet kijkt dan zijn alle nieuwsfeiten al weg die zakken al naar onder, die zakken al naar beneden, dus je moet dan al naar beneden te scrollen om te kijken.

J2: Ja of iedere dag kijken.

J1: Ja de meesten komen daar niet eens aan toe en ikzelf ook niet.

J2: En ik ben een staffer.

J1: Dus wij zoeken ook heel erg naar hoe kan je nou gewoon die zorgprofessionals aan het bed helpen dat die makkelijk maar ook op een ludieke manier want vaak denk ik dat ludiek communiceren dat blijft hangen en zo serieus dat blijft niet hangen dat is teveel en met dit onderwerp wat ook saai en taai is en noem maar op hebben wij eigenlijk iemand nodig die heel creatief van geest is die snapt waar de materie privacy over gaat en die daar een goede kwinkslag aan kan geven.

J2: Want ik zou best kunnen Twitteren ook als security officer waarbij ik hopelijk heel veel patiënten zou kunnen bereiken als we dat op een goede manier zouden doen dan is dat nog niet eens zo verkeerd. Maar dan heb ik daar wel hulp bij nodig dan moet iemand zeggen van 'goh zullen we dit eens Twitteren of zullen we hier aandacht aan besteden?' En dan wil ik dat best vanuit mijn profiel doen. Ik moet bijna een cursus twitteren hebben vanuit een bedrijfssetting zoals een ziekenhuis is want ja wat doe je wel en wat doe je niet. Ik doe het liever niet dan wel, ik vind het eng om te Twitteren als security officer. Ik denk ik kan het me niet permitteren als ik een foute tweet het huis in stuur. Dus ik doe het dus maar niet. Het is een veilige keuze dat snap ik ook, maar eigenlijk zou je willen dat ik wel die stap meemaak en dat ik ik Facebook niet want daar ben ik tegen, dus ik vind dat ik dat als security officer ook zeker niet moet doen, maar als ziekenhuis hebben we wel een Facebookpagina en daar zou ik misschien best gebruik van kunnen maken om onze patiënten te informeren. Dat we zeggen wij zijn een opleidingsziekenhuis dat betekent uw data zijn in principe alleen voor behandelaars etc.

RS: Maar hoe zit de communicatieafdeling nu dan in elkaar?

J2: Er zit gewoon een hoofd en er zijn een paar adviseurs die stand-by zijn een soort accountmanagers voor de organisatie, dus we hebben één vaste.

RS: Oké dus de vaste is degene die bepaalt wat er gaat gebeuren?

J2: Ja, en die anderen zijn meer voor nood als er een dienst is of als er een crisis is en dan hebben we nog een medewerkster die echt alleen maar de social media doet. Maar die doet ook maar wat iedereen aangeeft dat is niet iemand die mij gaat helpen.

J1: Ik had dit weekend voor het eerst wat irritant dat nu weer die vacature voorbijkomt. En dan gebeurt er iets niet goed vind ik met social media. Als ik denk van alweer dan gaat er iets niet goed in je systeem.

J2: Ik denk echt als je het hebt van wat zou communicatie kunnen doen in ondersteuning van dit onderwerp? Zowel de medewerkers als naar de patiënten dus dat betekent dat je iets met die social media moet doen en via het portaal als patiënten hun informatie ophalen daar kun je ook teksten neer gaan zetten.

J1: Of dat je daar al een folder neerzet dat mensen kunnen zien hoe er met persoonsgegevens om wordt gegaan. Dat mensen het aan de voorkant al kunnen lezen.

J2: Ja, maar dat zijn de mensen die netjes via de DIGID inloggen in het portaal en dat kan ook nog niet iedereen. We hebben een grote vergrijsde bevolking hoe gaan we daar nu mee om? Kinderen die het voor hun ouders willen regelen, vrouwen voor hun man, voor hun kinderen, kinderen die een speciale positie hebben in deze wetgeving wat wel en niet mag ik vind dat een lastige materie hoe gaan we dat nou vormgeven?

RS: Ja, dus dat is eigenlijk een lastig punt om al die verschillende groepen te benaderen.

J2: Ja en wij gaan nu naar een nieuw CISEPD. Daar willen we een nieuwe CIS onder zetten. Dat betekent dat je hele strikte autorisatieprofielen daarop moet zetten. Dat moet je zelf leren kennen, maar je moet het eigenlijk ook gelijk communiceren, dus je moet daar iets mee. Dat voel ik ook. Ik heb tegen de projectleider ook gezegd er moet een goed communicatieplan op.

J1: Ik merk wel dat als je dan toch blogt en dan probeer ik een beetje het kopje aantrekkelijk te maken, ja dat hebben we wel geleerd. Dat je nieuwsgierig wordt, maar ik denk dat wij daar meer mee kunnen, maar dan kom je gewoon aan op het punt, wie kan je helpen om dat neer te zetten en wie faciliteert je dan een beetje ook in wat speelt er in de media?

J2: Hè je zou willen dat een communicatieadviseur zou zeggen ik ben dit tegengekomen in de media zullen we daar even wat mee doen? Bijvoorbeeld alle wachtwoorden zijn gehackt.

J1: Laten we op actuele dingen inspelen, maar dan heb je iemand nodig die volgt wat er gebeurt. Oh hee in dat ziekenhuis is dat gebeurt en dat is leuk dat wij er iets overheen doen hoe dat bij ons gaat.

RS: Want in hoeverre denken jullie dan dat communicatie een rol zou kunnen spelen in het inperken van de risico's?

J2: Ik denk dat zij als zij een actieve rol zouden vervullen dan kunnen zij heel veel doen in de preventie en op het moment dat je een crisis hebt kunnen zij curatief gewoon goed handelen.

J1: Wat misschien wel goed is om te melden is dat de afdeling communicatie een tijd lang zonder manager heeft gezeten en je merkt dan hoe zelfstandig is een team dan wel of niet? Hoe gaat dat verder. Nu zit er weer een manager op en ik denk dat dit soort zorgen waar wij nu tegenaan lopen dat die door deze nieuwe manager gewoon opgepikt moeten worden. En dat hij eigenlijk met een voorstel moet gaan komen van 'joh dit kunnen we bieden binnen de mogelijkheden dit niet' maar dan is het ook duidelijk. En dan weet je wel van bij wie moet ik voor wat zijn en hoe kunnen we het vormgeven.

J2: Ik bedoel we hebben best creatieve ideeën waar we wel eens over nagedacht hebben, maar waarvan ik niet het gevoel heb dat ik dat kwijt kan en dat iemand het oppakt. En dat is de samenwerking. Het is helemaal niet zo gek om bijvoorbeeld eens een brief te sturen naar alle patiënten over hoe wij omgaan met hun gegevens. Gewoon een brief op de mat heel simpel. Maar dat moet je bedenken en dat moet een keer ergens op komen te staan.

J1: Ja of dat je een soort algemene brief doet bij de krant.

J2: Maar dat zijn dingen waarvan je dan toch hoopt en dat is dan misschien nog wel leuk voor jouw onderzoek: ik zou best zoals wij NEN 7510 natuurlijk als kader hebben voor maatregelen die we kunnen nemen, zou ik eigenlijk best een soort handvat willen hebben vanuit de communicatie en voor communicatie. Hoe kunnen wij dit domein aanvliegen en wat zouden de dingen zijn die ons kunnen helpen om de bewustwording van de patiënt en de medewerker te vergroten.

J1: En je leveranciers eigenlijk.

RS: Ja dat is natuurlijk ook waar we met behulp van dit onderzoek aan werken om zo'n kader op te kunnen stellen voor de zorgsector.

J2: Dus ik denk dat we het wel weten, dus we zijn bewust onbekwaam, want wij zijn niet bekwaam in communiceren. Daar hebben wij een specialist bij nodig en daar hebben jullie voor geleerd. Voorbeeldbrieven, gewoon handvaten. Dus dat is denk ik samenvattend. Ik denk dat we zelf al heel veel gedaan en bedacht hebben, wij waren één van de eerste met een e-learning, dus het is ook niet zo dat we daar nou in stil hebben gezeten zal ik maar zeggen. We zoeken wel naar mogelijkheden om die bewustwording te vergroten. En ja het onderwerp wordt door de media natuurlijk ook meer onder de aandacht gebracht, dus dat helpt ons ook.

RS: Nou ik denk dat ik voldoende informatie heb. Heel erg bedankt voor het interview.

Nagesprek

5.11 Uitwerking interview zorginstelling K

RS: Hoe ben je bij de functie terechtgekomen, want het is natuurlijk vrij nieuw de functie van functionaris gegevensbescherming. Hoe is dat zo gekomen?

Zorginstelling K: Ik werk zelf al meer dan 20 jaar in dit vakgebied en dat is informatiebeveiliging en privacy. Deze instelling heeft vier/vijf jaar geleden een functionaris gegevensbescherming aangesteld. Daar hadden ze toen een project voor ingeregeld om dat structureel vorm te geven. Toen hebben ze die functie gecreëerd en een collega van mij in die functie aangesteld. Die collega heeft mij drie/vier jaar geleden gevraagd om hem te helpen de informatiebeveiliging en privacy beter vorm te geven in dit huis en zo ben ik in zijn team terechtgekomen. En mijn collega is kortgeleden van baan veranderd, dus ik pak nu eigenlijk zijn rol even over, maar formeel hebben we een andere functionaris gegevensbescherming. Dat is iemand die tijdelijk als interim is benoemd en hij probeert zich hierop in te werken, dus eigenlijk pak ik de taken en activiteiten over van de functionaris gegevensbescherming, omdat ik inhoudelijk degene ben met de kennis en de ervaring ook in het huis hoe we hiermee om moeten gaan.

RS: Dus jij zit dan meer op het vlak van hoe gaan we er in de organisatie mee om en degene die hier nu ingewerkt wordt op het vlak van de toezichthouder.

Zorginstelling K: Nee, hij was tot voor kort de directeur ad interim in dit huis voor informatietechnologie en informatieverwerking en is gevraagd door de Raad van Bestuur om tijdelijk deze rol waar te nemen. We zijn op dit moment bezig om de hele informatiebeveiliging en privacybescherming beter vorm te geven op verzoek van de Raad van Bestuur, ook in opdracht van de Raad van Bestuur en we proberen daar een duidelijke scheiding te krijgen over wat gaat nu over informatiebeveiliging en wat gaat over die toezichthoudende rol? Hoe moet je dat nou goed vormgeven en waar moet je dat nou goed beleggen? Het ligt nu beide bij de staf van de Raad van Bestuur en daar komt een splitsing in en hoe dat precies nog vorm gaat krijgen is nog een beetje onduidelijk.

RS: Dus op dit moment zitten jullie in de bestuursstaf. En je zei in het team van functionarissen gegevensbescherming terechtkomen, zijn daar meerdere mensen?

Zorginstelling K: Jazeker, we hadden een team informatiebeveiliging en privacy van twee man, waarbij de leidinggevende rol beide rollen had zowel functionaris gegevensbescherming als centrale coördinator informatiebeveiliging. En die twee rollen daar zie je nu dat daar een splitsing in komt want het is lastig om zowel toezicht te houden op hoe je omgaat met de bescherming van persoonsgegevens en ook proberen te regelen dat het goed gebeurt in het huis. En die CISO rol is meer hoe regel ik nu met het huis dat we die gegevens goed beschermen en de andere is doen we het wel op de juiste manier?

RS: Ja, want je hebt natuurlijk privacy en je hebt de bescherming van persoonsgegevens maken jullie daar ook onderscheid in?

Zorginstelling K: Voor mij is de brede rol ik bescherm de informatie die voor dit huis belangrijk is en één van die gegevens die we moeten beschermen zijn de persoonsgegevens, maar dat is dus heel breed. Je hebt hier discussies over van als ik de naam eruit haal dan heb ik geanonimiseerde gegevens want de naam is weg. Terwijl ik zoiets heb van ja maar wacht even uit de andere gegevens kan ik afleiden wie die persoon is. Dus het is indirect herleidbaar. Nou de CISO-rol is zeg maar heel breed van hoe bescherm ik die gegevens: wat voor maatregelen moet ik treffen, hoe communiceer ik daarover? En de FG heeft veel meer de rol van zijn die maatregelen effectief en doen we de juiste dingen? En als het fout gaat wat leren we ervan om te zorgen dat de gevolgen voor de betrokkenen beperkt blijven? En ik richt me dit jaar eigenlijk voornamelijk op dat FG werk: hebben we het goed geregeld, wat gaat er mis en wat kan ik daarover vertellen en wat communiceer ik naar het huis om dingen te verbeteren en die CISO-rol schuif ik eigenlijk door naar iemand die meer in de IT-organisatie zit, die wel zaken oppakt en probeert daar de juiste maatregelen te vinden.

RS: En het was in opdracht van de Raad van Bestuur om die persoon aan te stellen die daar nu ook mee beziggaat. Hoe hebben zij dit thema in beeld?

Zorginstelling K: Het staat nu in de top 5 bij de Raad van Bestuur. Ze vinden het heel erg belangrijk en de verantwoordelijke in de Raad van Bestuur hamert er ook op bij mijn collega dat we stappen moeten maken. Wat kunnen wij nog meer doen? Hoe kan ik daar beter op sturen? We doen bepaalde dingen. De zorg heeft net de kranten gehaald met er zijn zoveel datalekken en haar vraag is van doen we het nou goed, hoe kan ik beter sturen? Nou dat is dus ook dat communiceren naar haar van wat kan ik aan haar laten zien zodat zij het gevoel krijgt van ja we gaan de goede kant op of hee ik wil bijspringen.

RS: Ja, want wat doen jullie op dit moment al aan beleid? Wordt dat dan door jou opgesteld of door de Raad van Bestuur?

Zorginstelling K: Het team dat zich bezighoudt met informatiebeveiliging en privacy stelt in zijn algemeenheid het beleid op, dus we hebben een informatiebeveiligingsbeleid en een stukje rondom privacy opgesteld en dat proberen wij steeds met nieuwe stukjes tekst en beleid te vertalen naar iets wat het huis kan gebruiken. Je ziet alleen dat in de zorg de mensen gewend zijn om bijna voorgeschreven te krijgen hoe zij wondbehandeling moeten doen. En dat noemen zij op een gegeven moment wat is het beleid ten aanzien van de wondbehandeling? Wanneer moet ik verschonen, pleisters plakken, verband leggen noem maar op. Als je kijkt naar informatiebeveiliging dan zeggen wij hier moet je over nadenken en dit is de richting waar je wilt komen, terwijl de zorg veel meer heeft van zo moet ik het uitvoeren. Dus daar zie je een discrepantie in het woordje beleid van wat ermee bedoeld wordt. Dus wij proberen van dat algemene kader wat wij als ziekenhuis moeten volgen, de NEN-7510, dat hebben wij verder uitgewerkt in meer concrete stappen die in het huis genomen kunnen worden van oké hoe ga je informatie beschermen? En vervolgens zijn we bezig om te kijken oké hoe gaat dit landen in al die afdelingen die dit uiteindelijk moeten uitvoeren?

Eén van de lastige punten is dat er een heleboel wet- en regelgeving naar beneden komt vanuit de overheid en vanuit de maatschappij van hier moeten we als ziekenhuis aan voldoen. En wij komen meestal on-top-off dus er zijn al een aantal dingen ingeregeld en dan is het van 'oja daar heb je die jongens van beveiliging weer die zeggen dat het beter moet'. En dat is continu communiceren; het gaat om persoonsgegevens wat kun je er wel mee doen en wat niet, neem die afweging van kan dit wel of kan dit niet. En dat stukje is voor iemand in de zorg lastig. Want die is namelijk gewend om te horen ik moet links of rechtsaf gaan in plaats van ik moet erover nadenken. Dus we hebben algemeen beleid in Nederland e-mail is niet veilig, dus patiëntgegevens mogen niet in de e-mail, maar als de patiënt nu op een operatietafel ligt en ik moet bepaalde informatie bij die arts proberen te krijgen dan kan ik het natuurlijk wel via allerlei media bij die arts krijgen, maar het is dan niet op dit moment bij die arts, dus je kunt hem opbellen, je kunt hem smsen, maar je kunt hem ook een e-mail sturen. En dan is dus de afweging op dat moment: hoe belangrijk is het dat de arts deze informatie heeft ten opzichte van ja maar misschien verlies je wat privacy. Nou die afweging moeten ze leren maken en dat is een andere insteek, dus dat is heel veel praten met, uitleggen, toelichting geven en dit soort gekke voorbeelden gebruiken.

RS: Ja, want ben je dan ook bekend met de 'ZEKER' campagne van de NVZ? Dat was onderdeel van de Alert Online weken.

Zorginstelling K: Nou wij zijn niet aangesloten bij de NVZ, omdat wij een UMC zijn. Ik heb er wel wat van meegekregen van mijn collega die er wel naar kijkt. We hebben wel eens dat kader ook binnen dit huis een campagne gestart om een stukje bewustwording weer even onder de aandacht te brengen van nou we hebben een securityweek gehad en als gevolg daarvan hebben we ook weer een campagne van welk middel moet je wel inzetten en wat moet je niet doen? En wees bewust waar je op klikt.

RS: En hoe wordt dat dan gecommuniceerd binnen dit huis?

Zorginstelling K: We hebben voor die campagne heel duidelijk gezegd, vanuit de directie meteen, dat er deze keer een campagne gevoerd moet worden. Jullie hebben een aantal middelen en vertel die gebruikers nou eens een keer wat ze wel en wat ze niet moeten doen, want er zitten randvoorwaarden aan het gebruik van IT en communiceer daar een keer over. En dan zie je dat dat wel een lang traject is geweest om dat in gang te zetten, maar uiteindelijk hebben ze ook gezegd: 'ja dit vinden wij belangrijk want wij hebben er ook last van'.

Als IT-leverancier hebben wij in dit huis op het moment dat gebruikers te vaak op de verkeerde dingen klikken. Allemaal dingen die wij niet willen hebben en moeten verbeteren. Bestanden worden weggegooid, kunnen we weer terugzetten. Klikken op mailtjes waarvan we zeggen ja wat is dit voor mailtje? Nou dan vervolgens moet de IT-club dat weer allemaal verbeteren, dus die hadden op een gegeven moment zoiets van laten we dat nou voorkomen voordat dat bij ons zover is. En dat is dan wel weer leuk. Je leert van de fouten van anderen.

RS: Ja, van de fouten die gemaakt worden.

Zorginstelling K: Je ziet andere ziekenhuizen hadden op een gegeven moment ergens last van en dan was het bij ons zo van 'ja wacht even zij hebben daar last van wat gaan wij doen om te zorgen dat wij dat niet krijgen?' En dat zet iets in gang, dus we hebben nu ook vanuit de Raad van Bestuur op een gegeven moment aangegeven: jongens er moet iets komen zoals een e-learningmodule, zodat gebruikers zodra ze binnenkomen die module kunnen volgen zodat ze in ieder geval de basis kennen.

RS: Ja en wordt er dan ook op dit moment al op afdelingen gesproken over dit thema? Staat het bijvoorbeeld op de agenda van overleggen?

Zorginstelling K: Voor zover ik weet wel. Eind vorig jaar zijn we begonnen met wat moeten we allemaal doen rondom de Meldplicht Datalekken. Op dat moment hebben we met z'n tweeën gezegd ja we moeten via de Raad van Bestuur gaan communiceren met het huis, dus we hebben wat teksten gemaakt voor de Raad van Bestuur. Dit komt eraan en wij verwachten dat wij dit en dit gaan doen als huis. Als er iets mis is, meld het aan bij ons. We hebben vervolgens gezorgd dat er een aantal systemen ingericht zijn en dat er een mailbak is gekomen zodat mensen informatie kwijt kunnen als 'hee ik heb iets gezien wat niet klopt'. Die pak ik op dan bel ik de mensen op om samen met de mensen te kijken wat is er aan de hand? En om dan vervolgens te zeggen is dit wel of niet een datalek en wat ga ik daarmee doen? In dat kader hebben we ook de eerste helft van het jaar zijn we zelf de organisatie ingegaan met presentaties in de afdelingen bij MT's van de divisies om te vertellen wat is nou informatiebeveiliging wat betekent privacy en wat moet je nou doen als iets niet goed gaat? En wat zijn de vuistregels? Wat doe je wel en wat doe je niet? Zo hebben we ook een aantal divisies die dit zelf opgepakt hebben, die hebben we in het begin meegenomen en gezegd: 'Ja dit kost ons veel tijd kunnen jullie helpen?' Nou een aantal zeiden nou jullie doen dat en deze heeft gezegd: 'wij pakken dit op'. En die hebben gewoon twee medewerkers dedicated op dit stuk gezet en die gaan dus bij hun eigen divisie langs alle afdelingen om te vertellen wat er aan de hand is met informatiebeveiliging, wat je moet doen om tot een selectie te komen van de juiste maatregelen en hoe je een risicoanalyse uitvoert. Betrek de mensen van centraal erbij omdat dat de experts zijn. Medewerkers komen vervolgens terug met vragen vanuit de presentatie en wij halen de antwoorden erbij van wat kan wel en wat kan niet. Dat communiceren we terug en dat wordt weer meegenomen in zo'n cyclus. Dus je ziet dat er nu heel veel aandacht wordt besteed in deze divisie aan het moet beter.

RS: Want is er dan een procedure ingericht voor de Meldplicht Datalekken?

Zorginstelling K: Ja, we hebben een procedure ingeregeld. Op zich is het heel eenvoudig het zijn ook een paar hele simpele stappen. De persoon die het ziet kan het bij ons melden via een aantal kanalen ze kunnen mailtjes sturen, ze kunnen ons opbellen, ze kunnen het melden in het incidentmeldingssysteem. Wij pakken de meldingen dan op, nemen contact op met die mensen, bepalen vervolgens met de informatiemanager van die divisie wat er nou specifiek aan de hand is en kijken vervolgens wat er moet gebeuren. Wij voeren de coördinatie op het hele traject om te kijken of wij de juiste dingen hebben gedaan. Melden we op tijd bij de Autoriteit Persoonsgegevens, melden we op tijd bij de betrokkenen, hebben we het goed voor elkaar en kunnen we daar ook bijspringen?

RS: En speelt de Raad van Bestuur daar dan ook een rol in?

Zorginstelling K: Nou wij zijn feitelijk staf van de Raad van Bestuur, dus eigenlijk doen wij dat namens de Raad van Bestuur. En dat is een vrij eenvoudige beslissing vind ik op het moment dat er persoonsgegevens bij

betrokken zijn meld je in ieder geval bij de AP en als het dan ook nog persoonsgegevens zijn die niet adequaat zijn beveiligd ga je dus ook nog eens een keer naar de betrokkene.

RS: En je zei net dat er informatiemanagers zijn, iedere afdeling heeft een informatiemanager?

Zorginstelling K: Nou we hebben een aantal directies, dat is meer ondersteunend die leveren geen primaire zorg en dan hebben we een aantal divisies en die leveren echt de zorg. En dan heb je een aantal divisies waarvan je zegt die komen direct in contact met de patiënt daar komt de patiënt binnen dus interne geneeskunde, de hart en longen, dat zijn poortdivisies dus daar kan een patiënt binnenkomen en dan heb je meer ondersteunend, die wel betrokken zijn bij het leveren van zorg, maar waar de patiënt in principe niet binnenkomt bijvoorbeeld biometische genetica. Deze divisies hebben allemaal een informatiemanager en de directies hebben er ook één en die worden dan ondersteund door een ICT-coördinator en functioneel beheerders, die hun eigen taken hebben in dat hele organisatieproces: het uitrollen van de middelen en het helpen van de eindgebruikers.

RS: Ja en informeren jullie dan die mensen zijn jullie dan het centrale aanspreekpunt?

Zorginstelling K: Voor die datalekken zijn wij het centrale aanspreekpunt dus dat komt primair eerst bij ons en dan gaan wij het verspreiden want het kan zijn dat incidenten wel door de ene worden gezien, maar voor een hele andere divisie zijn. Nou dan weten wij op een gegeven moment ook wel van deze persoon van divisie A heeft het gezien en dit moet dus naar divisie B of naar de directie, dat kan goed gebeuren en dan proberen wij een beetje te coördineren. En dat gaat soms nog wel eens mis, dat wij denken van oh dat hoort bij die divisie en dan blijkt het toch een verhuizing te zijn, waarvan je dan plotseling zegt van oh wacht even het ligt bij een andere.

RS: En wat zijn voor jullie als instelling dan risico's of mogelijke gevolgen van een beveiligingsincident of datalek?

Zorginstelling K: Als je gewoon goed kijkt naar het ziekenhuis dan denk ik dat de belangrijkste verstoringen eigenlijk de stroom zijn en nog de ondersteuning. Je hebt daar natuurlijk wel de maatregelen voor, maar we hebben stroomstoringen, storingen in de infrastructuur en dat patiënten hier niet meer kunnen komen dat zijn voor ons de dingen waarvoor je maatregelen treft. En als je dan gaat kijken naar ondersteunende informatiesystemen dan hebben we een aantal kernsystemen die mogen eigenlijk niet uitvallen. Het registratiesysteem is eigenlijk helemaal niet zo belangrijk, maar zorgen dat medewerkers weten waar ze moeten zijn als de dag begint als de planning overhoop ligt dan staan ze allemaal in de gang dan weet je niet wat je moet doen. Dus op die manier kijken we van wat zijn voor ons nou kritieke systemen en hoe gaan we dat implementeren? En dan kom je met de maatregelen. Dus afgelopen twee drie jaar zijn we ook echt bewust bezig geweest met het doorvoeren van veel meer risicoanalyses en de divisies bewust maken van oké hoe maak je die inschatting? En dan komen ze dus inderdaad met een nieuw systeem: hoe gaan we het gebruiken? Hoe ga ik het inzetten? Wat voor soort informatie komt erin? Kun je zonder deze informatie of heb je die continu nodig? En zo maak je inschattingen: nou dan zijn dit maatregelen die je kunt treffen en dan is het vervolgens aan de divisie om die keuze te maken van hoeveel geld wil ik daar uiteindelijk voor betalen.

RS: Ja, precies het speelt natuurlijk altijd mee wat het budget is, want jullie krijgen wel een bepaald budget van de Raad van Bestuur?

Zorginstelling K: Nou we hebben wel budget, maar dat ligt vooral in de divisies, dus die moeten redelijk zelfstandig kunnen opereren en als die zeggen ik heb een MRI-scanner nodig en dat is een redelijk duur apparaat. Daar kun je één van aanschaffen en geen twee. Dat zijn toch vrij dure resources die ik nodig heb en hoe is die afweging. Wat moet ik daar omheen anders regelen als ik er maar eentje heb? En dat is toch echt helemaal aan de divisie zelf want die moeten de zorg primair leveren, maar eigenlijk ben je wel verantwoordelijk. Ze moeten hun broek zelf wel ophouden. Onze Raad van Bestuur heeft een besturingsfilosofie waarbij eigenlijk heel veel verantwoordelijkheid in divisies zit, want daar hebben ze ook het beste inzicht hoe ze dingen moeten doen.

RS: Ja, dat kan ik me voorstellen, omdat er natuurlijk heel veel verschillende afdelingen zijn. Want hoe doen jullie dat dan? Hoe zorgen jullie ervoor dat al die verschillende afdelingen worden bereikt? Hebben jullie daar verschillende manieren voor of doen jullie dat op dezelfde manier?

Zorginstelling K: Dat wisselt vrij sterk. Dat is afhankelijk van hoe een divisie er zelf mee om wil gaan. Er zijn bijvoorbeeld divisies die zeggen van doe voor ons een presentatie of een stukje tekst, maar we hebben een website waar we intern op kunnen publiceren, we hebben nieuwsbrieven die we kunnen publiceren met daarin: jongens dit speelt, dus hou daar rekening mee. En dan proberen we een beetje in te spelen op de actualiteit dat we zeggen van hee dit speelt en dan komt er een nieuwsberichtje en dan is dat soms vanuit de directie IT, omdat het wel handig is als zij dit doen, want gebruikers die hiermee werken kijken eerder bij hen dan bij ons.

RS: En dat is dan de directie die verantwoordelijk is voor de IT?

Zorginstelling K: Gewoon de IT-organisatie die zegt: 'We hebben hier last van, werk even op een andere manier of gebruik de noodprocedure om iets voor elkaar te krijgen'. En dan zie je dus dat de divisies daar vrij snel en makkelijk mee om kunnen gaan. Daar halen ze de informatie vandaan. En soms is het ook zo dat ze die informatie gewoon niet kunnen vinden. We hebben ook een centrale afdeling marketing en communicatie, die wij voor twee dingen kunnen inzetten. Heel direct en persoonlijk gericht op de persoon: de medewerker, de patiënt, de student of veel meer algemeen naar de kranten toe, de pers. En dat zijn ook weer twee vormen die je kunt inzetten.

RS: Ja, want werken jullie dan ook samen met de afdeling marketingcommunicatie om bijvoorbeeld een bewustwordingscampagne op te zetten?

Zorginstelling K: Nou de campagne zoals die nu loopt bij de directie IT dat is in samenspraak met de marketingadviseur en zij heeft het traject getrokken. We hebben gezegd van nou jongens dit gaat over communiceren met, niet ons vakgebied, wij zijn vakidioten. Dus jij snapt hoe je moet communiceren, zoek de juiste weg, vraag aan ons de inhoud, dan kunnen wij dat wel op die manier voeden. Dat heeft zij redelijk goed zelf binnen haar directie opgezet samen met de specialist gezegd: 'Dit is de boodschap die wij willen overbrengen'. En ze heeft dus een aantal dingen gemaakt die hier ook uitgedeeld zijn. Je ziet ze ook elektronisch, dus je kunt het nog opzoeken op het intranet.

RS: Dus het zijn een aantal middelen, ook folders, flyers?

Zorginstelling K: Het zijn niet echt folders het is zo'n geplastificeerd a4tje met een aantal spelregels erop met wat doe je wel en wat doe je niet. En die zijn door het huis verspreid en het is ook op de website geplaatst zodat medewerkers het daar vanaf kunnen halen en er zijn nog wat andere stukken tekst daaromheen neergezet om dit stukje bewustwording neer te zetten.

RS: Ja, want merk je bijvoorbeeld sinds de Wet Meldplicht Datalekken is ingevoerd dat mensen er meer mee bezig zijn?

Zorginstelling K: In zijn algemeenheid gezegd er zijn iets meer dan 4500 datalekken gemeld. In de zorg zijn er iets meer dan 300 gemeld en als ik een beetje kijk hoe wij als huis acteren steken wij met kop en schouders boven de andere huizen uit. En niet omdat wij zo slecht of goed zijn, maar de bereidheid om hier meldingen te doen en met vragen te komen van hee wat doe ik nou goed? Is dit nu wel of niet een datalek? Ik krijg denk ik wekelijks wel vijf tot tien vragen met betrekking tot hoe moet ik bepaalde dingen doen of ik krijg een verzoek om bepaalde gegevens aan te leveren, mag ik dat wel?

RS: Dus zij zijn er wel mee bezig om die vragen te stellen.

Zorginstelling K: Ja, medewerkers echt vooral op de werkvloer die daadwerkelijk dingen moeten doen die komen met vragen hee maar wacht even ik doe het zo, kan dat eigenlijk wel? En: kan ik het anders doen of kan ik het beter doen? En dat is echt toegenomen.

RS: Ja, dan kan je daar natuurlijk ook op acteren door beleid aan te passen. Dus medewerkers zijn daar meer mee bezig. En je hebt dan bijvoorbeeld zo'n campagne en dat gaat dan door het ziekenhuis heen, dus naar iedereen. En als je dan kijkt naar teamoverleggen, wordt het daar bijvoorbeeld op de agenda gezet of leveren jullie presentaties bij afdelingen?

Zorginstelling K: Wij hebben het eerste half jaar geventileerd van jongens we willen graag wat vertellen over dit onderwerp. We hebben het MT benaderd, de Manager bedrijfsvoering die dit in zijn portefeuille heeft, en gezegd: 'u kunt zelf een presentatie geven of wij komen toelichting geven in een teamoverleg'. En zo hebben we met zijn tweeën tien – vijftien afdelingen langsgelopen en mijn collega heeft er ook nog een aantal gehad, dus zo hebben we een aantal divisies bestookt met presentaties om dit tussen de oren te krijgen en je ziet ook dat dat soort divisies heel actief bezig zijn om na te denken over informatiebeveiliging en we hebben ook vanuit een aantal van die meldingen gezegd van wacht even we zien hier iets dat niet klopt in dit proces. Waar zit die verstoring eigenlijk? Dan kom je erachter dat er iets ergens niet klopt, een tabel klopte niet, en als je dat dan oplost dan zie je dat het aantal meldingen terugloopt, dan heb je dus de goede actie genomen.

RS: Ja, want waar zitten dan bijvoorbeeld lastige punten om groepen te bereiken? Bij GGZ-instellingen heb je bijvoorbeeld mensen die thuis werken en die zijn dan lastig te bereiken, komen hier ook zulke dingen voor?

Zorginstelling K: Ja, het is niet zozeer de locatie waar ze werken maar wel het specialisme. Je ziet dat er bepaalde divisies zijn die zijn zo bezig met een aantal grote trajecten om verbeteringen door te voeren dat ze zeggen: 'dit kan ik er nu niet bijhebben'. Daarnaast 'ik maak bijna alleen maar gebruik van standaardmiddelen dus als die standaardmiddelen goed zijn beveiligd dan hoef ik me niet zo druk te maken'. En zo heb je ook divisies die heel flexibel werken continu nieuwe dingen willen hebben en die zeggen: 'ja maar ik heb zoveel veranderingen, ik raak het overzicht kwijt. Kom me helpen om al die kleine dingetjes op orde te krijgen. Dus je hebt twee uitersten eigenlijk: degene die zegt als de techniek het maar doet dan is het oké vind ik want onze mensen werken zo weinig met informatie. Terwijl degene die contact heeft met de patiënten informatie moet uitwisselen over hoe ga je om met medicijnen die je gebruikt: moet het meer moet het minder? Of de mensen die chronisch hier langskomen dus regelmatig op bezoek komen, die wil je tussendoor ook kunnen informeren en daar hebben we een patiëntportaal voor. Dat hebben we juist gedaan om die communicatie naar de patiënt beter te maken en hij is veiliger dan alle andere manieren van communiceren, dus je ziet dat we daar eigenlijk gezegd hebben: hoe gaan we nu dat contact tussen patiënt en medewerker zodanig verbeteren dat we A effectiever zijn, dus dat het niet te lang duurt, maar dat het ook nog veilig is. En zo zie je dat als voorbeeld een traject waarbij de patiënt één keer per maand of één keer per zes weken terugkomt. Die vaste momenten komt hij terug, die verzamelt gedurende de periode zijn gegevens en in de bespreking zegt hij dit is er gebeurd in de afgelopen periode. Maar er wordt nu door artsen gezegd met de huidige stand van de techniek kan dat eigenlijk dagelijks of wekelijks, dan kan ik veel eerder ingrijpen, dus wordt gekeken naar een oplossing, maar dan wordt ook gezegd dat het wel veilig moet. Dat formuliertje kan de patiënt vergeten en dan krijg je wel een recapitulatie maar dan ben je niet volledig, dus je moet eigenlijk zorgen dat de integriteit en volledigheid van die gegevens beter wordt. Je zou het via de e-mail kunnen sturen, maar het zijn patiëntgegevens, dus liever niet via de e-mail, hoe dan wel? Dan krijg je daar dus dat er meer iets wordt gebouwd specifiek voor deze patiëntengroep waarbij je zegt ja en het is ook nog veilig.

RS: En zijn er nu bijvoorbeeld ook al maatregelen voor medewerkers als ze zaken niet melden?

Zorginstelling K: Ja, het ergste is als ze op straat komen te staan. Dus we hebben gewoon een sanctiebeleid of medewerkers bewust dingen doen die ze niet mogen doen, dan wordt vanuit de zorg gezegd hee wacht even dit zijn wel patiëntgegevens je was niet betrokken en je hebt wel zitten kijken we gaan afscheid nemen.

RS: Ja, dus daar zijn wel sancties aan verbonden. En als er dan bijvoorbeeld een issue is geweest wordt dat dan ook besproken of geëvalueerd?

Zorginstelling K: Voor zover ik ze kan overzien, want ik zit namelijk niet direct in dat stuk, omdat ik zelf ook zeg ik wil geen patiëntgegevens zien. Ik wil eigenlijk niet weten wat er gebeurd is op het moment dat je gaat kijken

of er iets vreemds is gebeurd dan zit ik meestal met de artsen om de tafel en dan blijkt meestal dat het systeem of de rapportage niet klopt en dat het toch gerechtvaardigd is. Op het moment dat het niet gerechtvaardigd is dan wordt het een gesprek tussen de behandelend arts en de medewerker en dat kan weer leiden tot ontslag. Maar dat is weer privacygevoelig voor de medewerker dus dat wil ik niet weten. Dat is voor mij heel duidelijk. Er zijn een aantal van dat soort no-go's waarvan ik zeg daar wil ik niet komen.

RS: Nee, precies dus dan hou je je daar bewust buiten en laat je het aan hen over om hiermee om te gaan. Want je hebt natuurlijk nu een soort tussenperiode. De Meldplicht Datalekken is ingevoerd en dan straks gaan we naar de Europese Verordening, die is natuurlijk al van kracht maar wordt nog niet gehandhaafd in 2018 kan er ook echt gehandhaafd gaan worden op die wet. In hoeverre denk je dat jullie hierop voorbereid gaan zijn tegen die tijd?

Zorginstelling K: Ik denk dat de hele zorgsector daar in zijn algemeenheid een groot probleem heeft, omdat je twee toezichthouders hebt: je hebt de inspectie gezondheidszorg en je hebt de autoriteit persoonsgegevens. IGZ stelt een aantal eisen waar je qua privacybescherming heel moeilijk aan kunt doen. Als je de kwaliteit van zorg wilt garanderen dan moet je ervoor zorgen dat informatie beschikbaar is. Aan de andere kant zegt de Autoriteit Persoonsgegevens: nee, alleen als jij de behandelend arts bent mag je bij de informatie. Nou die twee die staan op gespannen voet, want we zijn een UMC dus als een patiënt wordt behandeld, delen wij de informatie met de directe specialisten. Nou die zitten niet aan bed van de patiënt, dus de autoriteit zegt dat mag niet, maar de IGZ zegt het is voor de kwaliteit van de behandeling wel zo goed, want die mensen geven een stukje intervisie op deze patiënt en wat hier aan de hand is en die hebben een stukje ervaring die ze inbrengen waardoor de kwaliteit toeneemt. Daarnaast hebben we hier toch de bijzondere gevallen dus het zijn meestal multidisciplinaire behandelteams dus voor je het weet heb je in bepaalde trajecten 70 verschillende specialisten nodig, dat loopt gigantisch op.

RS: Want is het dan niet zo dat als je bijvoorbeeld wel onder het behandelteam valt, je dan wel die toegang mag krijgen?

Zorginstelling K: Nou als je in het behandelteam zit dan ben je direct betrokken bij de behandeling, maar het is veel meer van 'hee ik heb hier een patiënt en denk eens mee'. Voorbeeld we lopen hier met honderd cardiologen rond, daarvan komen misschien maar vijf aan bed met een normale dienst, maar die vijf willen wel met die andere vijfennegentig sparren over dit specifieke geval, want hier is iets bijzonders aan de hand. Want een normale patiënt kan ook in de regio behandeld worden, maar juist omdat het daar niet helemaal lukt komen ze hier. Dus het zijn wel bijzondere gevallen waar je alle kennis wilt mobiliseren die aanwezig is. Die 95 cardiologen komen dus niet aan tafel, maar die worden wel gebruikt als klankbord van doe ik als arts de juiste dingen? Nou IGZ zegt dat is toch wel nodig en AP zegt nou eigenlijk niet. Dat blijft lastig.

RS: Ja ik kan me ook voorstellen dat ze daar nog een rol in moeten gaan vervullen om dat beter te specificeren.

Zorginstelling K: Ja precies, dat gaan zij niet doen. Ze hebben vanuit het huis dat beter vormgegeven van zo werkt het en dat is getoetst tegen de Autoriteit Persoonsgegevens en die hebben gezegd dit is voor ons voldoende in ieder geval beter dan de andere huizen, maar er zitten nog punten van verbetering in. Dus je zou kunnen zeggen ik ga dat begrip behandelteam beter definiëren, zodat de toezichthouder op persoonsgegevens beter weet wat wij precies doen en dat IGZ ook zegt van wij snappen ook wat jullie doen. Dus voor een deel is het een stukje communicatie van hoe werk je met dit soort patiënten?

RS: Ja, ik kan me voorstellen dat het ook wel van belang is om een grote groep betrokken te houden bij de behandeling. Want hoe kijk je dan tegen die rol aan van de Autoriteit Persoonsgegevens? Heb je bijvoorbeeld informatie van hen ontvangen?

Zorginstelling K: Nou ik heb wel eens geprobeerd om de autoriteit zo ver te krijgen dat zij gingen sparren. Spiegelen van: 'jongens als we het zo inregelen is dat dan goed?' En uiteindelijk was het antwoord: 'ja maar we zijn geen kwaliteitsinstituut, we toetsen aan het eind of jullie iets goeds hebben gedaan de afgelopen periode'.

RS: Dus eigenlijk niet als adviseur willen optreden.

Zorginstelling K: Je krijgt ze niet als adviseur mee.

RS: En heb je dan contact met hen opgenomen of iets dergelijks om vragen te stellen?

Zorginstelling K: Nee, ze hebben op een gegeven moment een aantal onderzoeken gedaan in de zorgsector om te kijken hebben we het hier goed gedaan en toen zijn ze toevallig ook hier gekomen. En toen hebben we daar een aantal vragen neergelegd en hoe hebben we het gedaan. Nou uit dat onderzoek blijkt dat er één instelling in Nederland is die het regelt zoals de Autoriteit Persoonsgegevens dat wil en dat is een heel specifiek geval, dat is volgens mij een GGZ-instelling en daar was het op een bepaalde manier geregeld dat je inderdaad kon zeggen ja dit specialistisch stuk van zorg kun je op deze wijze inregelen. Dan heb je inderdaad een band tussen de behandelaar en de patiënt, dat is een één op één relatie. Als ik dat hier bij een harttransplantatie moet doen dan valt die patiënt op aan het eind van het behandeltraject. Want ja de ene na de ander die mag komen en die mag controleren bij een harttransplantatie ja dat gaat niet werken. Je hebt ze allemaal nodig en het liefst tegelijkertijd, dus dat is wel een spanningsveld. Het is wat overtrokken het voorbeeld maar dit is wel de discussie waar het om gaat.

RS: Ja, dus dat is eigenlijk nog iets waar nog meer duidelijkheid over zou moeten komen.

Zorginstelling K: Ja, maar dat is iets wat wij vooral vanuit de zorg denk ik duidelijk moeten proberen te maken aan deze twee toezichthouders.

RS: Want de IGZ die wil al die informatie wel? Want je hebt natuurlijk ook gemeenten en dergelijke en je hebt ketenpartners waartussen al die informatie wordt gedeeld. Want gemeentes willen ook veel dingen weten, hoe gaan jullie daar dan mee om?

Zorginstelling K: Dat weet ik gelukkig niet, want in dat stuk zit ik zelf niet. Gemeenten zitten op een andere plaats in de zorg. Wij werken vooral als tweede lijn, dus huisartsen en regioziekenhuizen besteden hun moeilijke patiënten aan ons uit. Vanuit ons gaat weinig informatie naar gemeenten voor zover ik dat kan overzien. Wel heel veel met zorgverzekeraars en huisartsen en andere kleine instellingen, maar meestal als tweede lijn achter die jongens.

RS: Ja, want dan moeten zij eigenlijk zorgen dat die gegevens naar jullie komen in plaats van andersom.

Zorginstelling K: Ja, dus wij geven wel als de patiënt is behandeld een stuk informatie in de vorm van een brief dat gaat terug naar de verwijzend arts, dus die wordt op deze wijze door ons geïnformeerd. Dit hebben wij met uw patiënt gedaan.

RS: Ja, dus op die manier wordt het wel teruggekoppeld aan hen. En als je dan kijkt naar meer extern hebben jullie bijvoorbeeld een extern meldpunt op de website? Waar ethische hackers of patiënten die iets opvalt in het ziekenhuis kunnen melden?

Zorginstelling K: Nou daar zijn we wel mee bezig om dat in te regelen, maar de UMC's die proberen dat gezamenlijk te doen en tot één systeem te komen, zodat we met zijn allen op dezelfde wijze responsible disclosure gaan invoeren. Ik weet wel dat wij op een gegeven moment een aantal berichten hebben gekregen van mensen die zeiden van hee dit is ons opgevallen wat moeten we hiermee en we hebben een CERT-team en ik heb gezegd: 'CERT-team willen jullie dit verder uitzoeken? Ik ken deze persoon niet. Neem contact op. Ga kijken wat er aan de hand is en ik hoor het graag'.

RS: Ja, precies, dus dan wordt het op die manier gedaan nu en dan wordt er algemeen iets geregeld tussen alle UMC's. Ik heb inderdaad ook al een aantal andere UMC's gesproken en daarin werd ook wel duidelijk dat er ook vaak gezamenlijk gekeken wordt naar hoe je het beleid kan invullen. Heb je daar dan een aparte vereniging voor voor UMC's, omdat ze dan niet bij de NVZ zijn aangesloten?

Zorginstelling K: Ja, dat noemen ze de NFU, Nederlandse Federatie voor UMC's. Vanuit die koepel heb je helemaal onderaan twee special interestgroups die zich bezig houden met informatiebeveiliging en privacybescherming.

RS: En als je meer kijkt naar de externe gevolgen dus bijvoorbeeld als je in het nieuws komt of iets dergelijks hoe gaan jullie daarmee om?

Zorginstelling K: Nou we hebben wel incidenten gehad en dat hebben ze hier redelijk voortvarend opgepakt. Ook in de communicatie van ons van wat wel en wat niet dus daar zijn ze dan wel vrij goed mee bezig. Daar hebben we dan ook een afdeling marketingcommunicatie voor die de regie vormt van als er wat gebeurt hoe gaan we daarmee om? Dan hebben we ook wel ons lesje geleerd uit voorgaande trajecten. Er komt behoorlijk veel druk op de medewerkers en dan is het nog steeds de vraag was het terecht of niet. En dan heb je daar onderling wel discussies over, die discussie blijft natuurlijk altijd wel gevoerd worden. Ik heb ook in de buitenkant gezeten, daar wordt ook altijd geroepen: altijd melden. Dus ik meld liever en dan haal ik dingen terug dan dat ik het niet doe. Maar er zijn inderdaad ook wel situaties dat de patiënt zelf iets aangeeft en dat is eigenlijk het moment dat ik wel in aanraking kom met de patiënt. Dat ze bij mij aankomen en vragen ja ik wil eigenlijk iets van het ziekenhuis en dat is via de normale paden niet gelukt, maar wat kun jij nu betekenen voor mij? En dan komen ze soms met hele vreemde eisen. Dat bijvoorbeeld wordt gezegd: 'mijn gegevens mogen met niemand gedeeld worden' of 'nee je mag mijn BSN niet gebruiken, je mag dit niet delen, je mag mijn naam niet weten'. En dan snap ik dat ze dat willen, want dat recht mag je hebben, maar helaas heb ik ook een aantal andere eisen en ik moet gewoon een aantal dingen vastleggen en registreren in het kader van die andere toezichthouder. Als ik bijvoorbeeld niet vastleg wat ik jou heb toegediend hoe weet ik dan of ik voldoende heb toegediend? Dan hebben ze gesproken met de artsen en afdelingshoofden en dan komen uiteindelijk bij mij van ja maar kun jij dan niet iets regelen voor me.

RS: Ja, want ik kan me ook juist voorstellen dat het in het belang is voor de patiënt om bepaalde informatie op te slaan in ziekenhuizen.

Zorginstelling K: Ja, dat klopt. De meeste patiënten die bij mij aan de deur komen die zeggen ik heb iets gezien en ik denk dat dat beter kan en ik wil graag meewerken. En kun je me helpen om dit voor mekaar te krijgen? Want artsen zeggen op een gegeven moment van ja maar dit is te moeilijk ik kan dat niet ik snap dat niet. Ze zijn heel goed als arts, maar dit is een ander onderwerp. Het staat niet primair op de lijst van dit moet ik oplossen, nee daarvoor hebben ze een concernstaf om dat te doen.

RS: Ja, want zijn er dan ook informatiefolders of iets dergelijks voor patiënten voor privacybescherming? Dat ze kunnen zien hoe er met hun persoonsgegevens wordt omgegaan?

Zorginstelling K: Ja, we hebben een algemene folder voor patiënten en daarin staat gewoon beschreven wat kan ik als patiënt verwachten en hoe gaan wij om met hun gegevens. Wat kun je wel verwachten en wat kun je niet verwachten? En bij een aantal dingen staat gewoon duidelijk uitgelegd van heb je vragen dan kun je daar naar toe en heb je klachten dan kun je daar naar toe. En we hebben dat patiëntportaal dus je kunt vrij direct zien wat wij vastleggen over jou als patiënt en daar kunnen ze zien wat heeft de arts vastgesteld.

RS: Nou ik denk dat ik een heleboel nieuwe informatie heb, dus dat is mooi daar kan ik weer mee verder. Ik heb verder in ieder geval geen vragen meer, ik weet niet of jij nog vragen hebt?

Nagesprek

5.12 Uitwerking interview zorginstelling L

RS: Eerst ben ik benieuwd hoe ben je bij deze functie terechtgekomen? Want het is natuurlijk vrij nieuw de functie van functionaris voor de gegevensbescherming.

Zorginstelling L: Mijn functie is oorspronkelijk beleidsadviseur Zorg en Kwaliteit. Ik ben hier acht jaar geleden begonnen met de opdracht om de HKZ-certificering te begeleiden en te coördineren en daarnaast ben ik ook

verantwoordelijk voor de AOIC (Administratieve Organisatie en Interne Controle). Dit heeft alles te maken met de inrichting van jouw zorgadministratie. Mijn rol daarin is om ervoor te zorgen dat alle productie zodanig gecontroleerd wordt dat we dat ook aan de accountants kunnen voorleggen, zodat zij daar een stempel op kunnen zetten. Dat is in oorsprong mijn functie. Van daaruit ben ik steeds meer inhoudelijke projecten gaan trekken zoals het invoeren van zorgprogramma's en zorgpaden. Eigenlijk toen die verplichting kwam dat we nu met informatiebeveiliging aan de slag moeten. We willen daarvoor ook voor certificering gaan. Toen is die vraag eigenlijk ook bij mij terecht gekomen, omdat ik van oorsprong gewoon projecten op mijn bordje heb die een soort kapstokkarakter hebben, dus vandaaruit kwam ik naar voren. En ik heb mijn collega informatiemanager geholpen dat op te zetten. We hebben de NEN-7510 gepakt en gekeken wat de normen zijn. En wat moeten wij nog doen als instelling om daaraan te voldoen? De eerste stap die we vervolgens hebben gezet is beleid ontwikkelen. En wat we eigenlijk niet wilden doen is er een apart riedeltje voor ophangen, dus we wilden zoveel mogelijk aansluiten bij het kwaliteitsmanagementsysteem dat we hebben vanuit de HKZ. Dus informatiebeveiliging is daar gewoon een onderdeel van geworden en we hebben gekeken van nou oké wat is ons beleid ten aanzien van informatiebeveiliging. Hoe kijken wij er tegenaan? Wat vinden wij informatiebeveiliging? Wat vinden wij belangrijk? En van daaruit zijn we verder gaan kijken naar de inrichting. En dat is eigenlijk anderhalf jaar geleden dat we daarmee zijn begonnen.

RS: Dus toen zijn jullie ook begonnen met het opstellen van beleid, want hoe heeft de Raad van Bestuur dit thema dan bijvoorbeeld in beeld?

Zorginstelling L: Informatiebeveiliging daar is de voorzitter Raad van Bestuur portefeuillehouder van. Het hoofd bedrijfsondersteuning is gedelegeerd opdrachtnemer en mijn collega informatiemanager die is degene die het project leidt binnen de instelling en ik ondersteun daarbij.

RS: En hoeveel uur per week ben jij hier dan mee bezig?

Zorginstelling L: Nou officieel hoor ik hier twee dagen per week mee bezig te zijn, maar ik denk dat ik eerder zit op vier uur.

RS: En wat hebben jullie dan bijvoorbeeld voor beleid opgesteld? Waar moet ik dan aan denken?

Zorginstelling L: Dan gaat het echt specifiek om de organisatie. Wie is verantwoordelijk waarvoor als het gaat om informatiebeveiliging? Wat is de rol van de Raad van Bestuur? Wat is de rol van de directie? Wat is de rol van de informatiemanager? Wat is de rol van de security officer? Maar ook wat is de rol van de lijn? Als zij iets signaleren wat niet goed gaat waar kunnen zij dat aankaarten. Dat is eigenlijk wat we in kaart hebben gebracht en beschreven. En wat we daarnaast hebben gedaan is kijken naar je hele IT-landschap, je hardware, je netwerk, je software, je applicaties. Als je kijkt naar de applicaties met name, wie is daar applicatie-eigenaar van en hoe verhoudt dat zich weer tot de besluiten die op dat punt moeten worden genomen als het gaat om wijzigingen of nieuwe applicaties aanschaffen. Dus de hele organisatie om informatiebeveiliging heen dat is in kaart gebracht en beschreven.

RS: Ja, een soort risico-inventarisatie?

Zorginstelling L: Nee, dat is de volgende stap die we hebben gedaan. We hebben eerst het beleid beschreven wie is waarvoor verantwoordelijk. We hebben daarna alles wat wij vonden dat te maken had met informatiebeveiliging in kaart gebracht en op basis daarvan hebben we vervolgens een risicoanalyse uitgevoerd van oké waar zitten wat ons betreft de grootste dreigingen en op basis van die dreigingen hoe groot is de kans dat een bepaald risico voorkomt? Op basis daarvan hebben we een risicoanalyse uitgevoerd.

RS: En voor jullie als instelling wat zijn dan bijvoorbeeld gevolgen waar ik aan kan denken als er wel een incident zou plaatsvinden?

Zorginstelling L: Nou ons grootste risico zit aan de zachte kant. Informatiebeveiliging heeft twee kanten een harde kant en een zachte kant. En de harde kant hebben we vrij goed ingericht denk ik. We hebben een deel van onze IT ook geoutsourcet en daar ook allerlei afspraken gemaakt met de leverancier. Maar wat je ziet is je

kunt je netwerk, je applicaties, wel goed beveiligen, maar als mensen zich daar niet aan houden bijvoorbeeld aan wachtwoorden, aan autorisaties, dan kom je ook niet ver. Die zachte kant dat is nog een risico wat ons betreft en dan kunnen het gewoon menselijke fouten zijn waardoor gegevens op de verkeerde plek terechtkomen of gegevens op de verkeerde plek worden opgeslagen of dat men zich gewoon niet bewust is van de afspraak dat je bijvoorbeeld niet je inloggegevens aan iemand anders mag afgeven, dus dat is wat ons betreft nu toch het grootste risico.

RS: Want zijn jullie dan bijvoorbeeld ook bekend met de 'ZEKER' campagne van de NVZ die in oktober gelopen heeft? Dat was onderdeel van de Alert Online Weken.

Zorginstelling L: Nee, ik heb dat niet meegekregen. Wat we wel hebben gedaan, we hebben vanuit onze koepelorganisatie GGZ-Nederland, die heeft ook zo'n awarenesscampagne opgezet, waar verschillende instellingen aan kunnen meedoen als ze dat willen. En daar zijn we nu wel mee bezig om naar het materiaal te kijken van hee is dat iets wat wij ook kunnen gebruiken en willen wij in dat traject meegaan?

RS: Ja, want hebben jullie verder al iets van communicatiebeleid opgesteld?

Zorginstelling L: Communicatiebeleid zo specifiek niet op het gebied van informatiebeveiliging, maar we zijn wel aan het nadenken hoe we die awareness bij medewerkers op gang kunnen krijgen. Hoe kunnen we mensen bewustmaken? Want informatiebeveiliging is gewoon een ver van hun bed show, maar de kunst is om het zodanig te vertalen dat het ook voor hen herkenbaar is. Bij ons hebben we te maken met patiëntenzorg dan komen behandelaren heel snel bij dossiervoering. Wat mag je van een dossier wel of niet meegeven aan een derde? Hoe ga je met autorisaties om? Mag je inloggegevens wel of niet verstrekken aan een ander? Als je op een scherm zit en je hebt een dossier openstaan laat het niet onbeheerd achter. Dus we zijn naar de awareness aan het kijken. We hebben een e-learning ontwikkeld daarvoor, die mensen kunnen gaan volgen. Dat is denk ik iets van drie uur dat ze dan een aantal vragen kunnen doorlopen, maar echt de campagne zelf die moeten we nog gaan opstarten.

RS: Oké dus ze kunnen al wel een e-learning doen, is dat verplicht? Moeten ze die al gedaan hebben?

Zorginstelling L: Ja, het is maximaal drie uur dat het in beslag neemt, maar we hebben geen periode eraan gekoppeld met en dan moet het gedaan zijn. Het is gewoon als er tijd voor beschikbaar is dat ze dat moeten gaan doen. En zolang ze dat niet hebben gedaan zie je dat ook niet in het systeem geregistreerd zeg maar.

RS: En wat staat er dan bijvoorbeeld in die e-learning? Wat leren ze dan?

Zorginstelling L: Nou die dingen die ik net al noemde bijvoorbeeld als je je computer hebt openstaan en er staat een patiëntdossier open en je verlaat je kamer: mag dat? Dat soort dingen staan daarop: autorisaties, wachtwoordbeleid, hoe vaak moet je wachtwoorden wijzigen? En dat je wachtwoorden niet op een papiertje opschrijft. Dat soort onderwerpen komen erin naar voren.

RS: Want hebben jullie die e-learning zelf ontwikkeld?

Zorginstelling L: Nee, we wilden dat wel, maar dat zou gewoon veel te veel tijd in beslag nemen, maar nee dat hebben we niet zelf ontwikkeld.

RS: Oké, nee want ik heb inderdaad ook een aantal bedrijven gesproken en ken er ook eentje die heel erg met e-learning bezig is. Die hebben allemaal verschillende thema's bijvoorbeeld phishing als thema, wachtwoordbeleid.

Zorginstelling L: Ja en volgens mij als je de verschillende e-learnings naast elkaar zet dan zullen de thema's ook elke keer terugkomen, want daar gaat het ook eigenlijk om.

RS: En als je dan kijkt naar wat meer externe gevolgen van bijvoorbeeld een datalek, wat zijn dan voor jullie belangrijke dingen?

Zorginstelling L: Ja, dan heeft het toch te maken met het feit in hoeverre ons netwerk beveiligd is en wat ik net al zei dat hebben we geoutsourcet en met hen hebben we gewoon afspraken gemaakt dat zij dat goed monitoren en moeten volgen en wij zitten met hen structureel om de tafel om te kijken wat er uit hun controles komt of zij dingen tegenkomen waar wij iets mee moeten.

RS: Ja, en sinds de Meldplicht Datalekken is ingevoerd, merk je dan ook verschil in de organisatie? Dat medewerkers er meer mee bezig zijn bijvoorbeeld?

Zorginstelling L: Nee, medewerkers zijn er totaal niet mee bezig. Nee, dat staat echt nog in de kinderschoenen. Wij proberen dat wel voor te bereiden en te ontwikkelen, maar medewerkers op de werkvloer als je die zou vragen, dan denk ik nee.

RS: Nee, want is er dan bijvoorbeeld al een procedure opgesteld voor datalekken als je iets signaleert?

Zorginstelling L: Wat we hebben gedaan, en dat is eigenlijk ook onderdeel van de NEN-7510, is het melden van incidenten. Dat hebben we wel gecommuniceerd. Daar hebben we wel een procedure voor opgesteld. We hebben een a4 opgesteld van incidenten die bijvoorbeeld en ook weer aan de hand van die vaste thema's: wachtwoordenbeleid, autorisatie, phishing, internet als je rare dingen in je e-mail tegenkomt. Dan hebben we een a4 opgesteld en gezegd als je rare dingen tegenkomt meld het dan. We hebben een veilig-incidenten-melden-systeem en daar hebben we informatiebeveiliging een onderdeel van gemaakt. Dus als mensen bijvoorbeeld bij de printer een dossier met gegevens van de patiënten zien liggen dan moeten ze dat gaan melden. Dan komt dat bij mij, de informatiemanager en bij de manager van degene die het heeft gemeld en dan wordt dat geanalyseerd en dan kijken we van hee hoe komt het nou dat dat kan gebeuren? En zo proberen we dat wel langzaamaan bespreekbaar te maken.

RS: Ja, want de manager krijgt daar dan ook meteen bericht van dat er iets is gebeurd en hoe gaat dat dan verder in zijn werk?

Zorginstelling L: Dan is het aan de manager om te beoordelen samen met ons of het een hoog risico incident is: wat zijn de gevolgen ervan? En als dat zo is dan moet op Raad van Bestuursniveau worden besloten wat we daaraan gaan doen. En als het iets is dat bijvoorbeeld ligt aan een menselijke fout of dat het een eenmalig iets is dat probeer je dan samen met elkaar in te schatten. En als het bijvoorbeeld te maken heeft met het feit dat de medewerker niet op de hoogte was van een bepaalde instructie, dan wordt het alsnog met het team besproken. Dus dan probeer je het met het team zelf op te lossen dat die fout daarna niet meer kan voorkomen.

RS: Nee, nee precies. Want zijn er dan al meldingen geweest ook naar de autoriteit?

Zorginstelling L: Niet naar de autoriteit, wel gewoon intern hebben we meldingen gehad. Dus dat zie je wel gebeuren dat sinds we dat hebben ingevoerd in het systeem dat mensen wel meer gaan melden. Dus mensen worden zich bewuster van het feit oké ik mag niet zomaar gegevens verstrekken of bij de printer gegevens achterlaten of dingen op je bureau laten slingeren, daar worden ze zich wel steeds bewuster van.

RS: En als er dan sprake is van een melding of iets wat mogelijk een incident kan worden dan gaat dat altijd via de Raad van Bestuur die beslissen?

Zorginstelling L: Van alle meldingen, ook zorginhoudelijke meldingen, worden rapportages gemaakt, halfjaarlijks, je hebt maandelijkse rapportages en je hebt ook halfjaarlijkse rapportages en die worden standaard in het MT besproken. Dan wordt gekeken naar de bevindingen van hee wat zien we nou? De trend wordt besproken en dan ook eventueel de maatregelen die daarop genomen moeten worden. Dus dat wordt op dat niveau besproken met de Raad van Bestuur erbij.

RS: En van wie uit kwam dan bijvoorbeeld het idee om de functie van functionaris voor de gegevensbescherming in te voeren?

Zorginstelling L: Oorspronkelijk van ons Hoofd Bedrijfsondersteuning, want die zat er echt bovenop en die heeft het bespreekbaar gemaakt bij de Raad van Bestuur en zo is het gaan rollen.

RS: En hoe zien zij dit thema nu? Heeft dit nu een hoge prioriteit of zijn er andere thema's waar zij prioriteit aan geven?

Zorginstelling L: Ja, als ik heel eerlijk ben: het heeft niet de hoogste prioriteit nee.

RS: Ja, dat maakt het waarschijnlijk ook lastig om iets door te voeren.

Zorginstelling L: Nou ik kan de Raad van Bestuur en het MT wel meekrijgen, maar als je naar de praktijk kijkt, de werkvloer dan is dat bijzonder lastig om zo'n taai thema ook ingevoerd te krijgen. Want waar zij zich op de werkvloer druk over maken is mijn productie, de patiëntenzorg dat staat bij hen gewoon voorop en daar worden ze ook op aangestuurd. En dan komt informatiebeveiliging echt op een lager prioriteitsniveau te staan, dat is nog even duwen en trekken inderdaad.

RS: Ja, want staat het bijvoorbeeld wel op agenda's van teamoverleggen?

Zorginstelling L: Nee, sterker nog het veilig incidenten melden dat zou een vast agendapunt moeten zijn binnen teamoverleggen, maar daar komen ze niet aan toe joh. Ze zijn gewoon meer met de dagelijkse dingen op de werkvloer bezig dan met dat soort thema's.

RS: Ja, want werken alle medewerkers hier op locaties? Of zijn er bijvoorbeeld ook thuiszorgmedewerkers?

Zorginstelling L: Nee, we hebben geen thuiszorgmedewerkers. We hebben wel twee teams die mobiel zijn en naar patiënten toe gaan en dan doen we een soort outreachende zorg, maar het merendeel zijn het medewerkers die gewoon hier op locatie werken.

RS: En toen jullie dat a4 hebben opgesteld hoe hebben jullie dat dan overgebracht naar de medewerkers?

Zorginstelling L: Via de lijn. We communiceren altijd beleidsafspraken via de directie. De directie communiceert dat naar de managers en de managers moeten dat met hun team bespreken.

RS: Oké en dat gaat in overleggen?

Zorginstelling L: Ja, dat gaat in vaste overleggen. We hebben een overlegstructuur. Eén keer in de maand hebben we bijvoorbeeld het MT, daarna hebben we de eigen RVE's (Resultaat Verantwoordelijke Eenheden). We hebben drie RVE's dan wordt het in het MT van de RVE's besproken en daar zitten alle managers bij en die horen dat met hun eigen teams te bespreken in hun eigen werkoverleg.

RS: Maar het is niet zo dat het centraal gecommuniceerd wordt bijvoorbeeld?

Zorginstelling L: Ja, dat doen we ook. We volgen dan de lijncommunicatie, maar we hebben ook een intranet waarop we berichten plaatsen en dat doen we dan ook regelmatig, maar ja niet iedereen leest intranet, dus je bereikt denk ik echt een minimum aan medewerkers die dat dan gaan lezen.

RS: Ja, want zijn er dan bijvoorbeeld in het algemeen voor informatiebeveiliging al dingen opgesteld? Zoals posters?

Zorginstelling L: Nee, we hebben geen posters. Het enige dat we toen hebben gedaan is de berichten op intranet. We houden een FAQ bij en that's it. Voor de rest hebben we er geen grote communicatiecampagne aan gehangen.

RS: Nee, want hebben jullie hier een communicatieafdeling?

Zorginstelling L: Ja, we hebben wel een communicatieafdeling.

RS: Hoe zitten die bijvoorbeeld in de organisatie verweven?

Zorginstelling L: Je hebt Raad van Bestuur en je hebt daar een bestuursbureau met de bestuurssecretaris en communicatie valt onder de bestuurssecretaris.

RS: En jullie, vallen jullie meteen onder de Raad van Bestuur?

Zorginstelling L: Nou daar zit ook nog iets tussen, je hebt Raad van Bestuur, bestuursbureau, dat zijn de ondersteunende diensten en je hebt dan het stafbureau en je hebt het bedrijfsbureau dat zijn de staffers en dan in de lijn heb je dan drie RVE's, dan heb je de directies en dan heb je de managers en dan ga je naar beneden en wij zitten aan de zijkant. En ik zit in het stafbureau en mijn leidinggevende is het hoofd van het stafbureau en die valt onder Raad van Bestuur.

RS: En hoe heten jullie als afdeling?

Zorginstelling L: Gewoon stafbureau.

RS: Oké dus daar zit van alles in.

Zorginstelling L: Ja, we zijn met verschillende portefeuilles bezig op het gebied van zorg en kwaliteit. Dan moet je denken aan cliënttevredenheid, medicatiedwang en drang. Wij zijn zeg maar echt de beleidsmakers samen met de managers en de lijn daar zitten de uitvoerders die gaan het implementeren.

RS: En waar zitten dan bijvoorbeeld lastige punten denk je om dingen geïmplementeerd te krijgen?

Zorginstelling L: De veelheid aan dingen die gedaan moeten worden. Je ziet als GGZ-instelling word je bijvoorbeeld door een inspectie op de hielen gezeten. Je wordt door zoveel externe organen gevolgd en gemonitord en je moet aan zoveel externe eisen voldoen, waardoor het soms zo veel is dat we eigenlijk door de bomen het bos niet meer kunnen zien en dan wordt het gewoon te veel. En dan sneuvelt een onderwerp als informatiebeveiliging, want de andere zorginhoudelijke onderwerpen die zijn gewoon belangrijker. Nou sterker nog de financiële onderwerpen zijn belangrijker. Ik bedoel als wij onze productie niet halen, het geld niet binnenkomt, dan houdt het op als we geen nieuwe cliënten hebben. Daar worden onze behandelaren op gedrild en gestuurd dat ze de productie moeten halen en nieuwe cliënten moeten binnenhalen.

RS: Dus op die manier is het dan lastig om zo'n beleid als dit…

Zorginstelling L: Ja, om daar aandacht voor te krijgen.

RS: Zijn daar al ideeën over om bijvoorbeeld een campagne op te zetten?

Zorginstelling L: Nee, wat ik net al zei we zouden bij een campagne van GGZ-Nederland kunnen aansluiten om te kijken of we dat kunnen gebruiken. Aan de ene kant wil je geen grote campagne opzetten, omdat het iets van de mensen zelf moet worden, dus het moet niet een apart iets worden. En wat ik net ook al zei: je moet het herkenbaar voor ze maken en als je het herkenbaar voor ze maakt dan slaat het vaak beter aan dan als je daar een hele campagne voor gaat opzetten. Dus daar zijn we nog even naar aan het zoeken van ja wat is wijsheid? Willen we daar echt bijeenkomsten voor organiseren waar ze allemaal naar toe moeten gaan? Dat daar presentaties en workshops over plaatsvinden. Of wil je dat in de bestaande overleggen en structuren en systemen gaan uitrollen? Dus dat zijn vraagstukken waar we nog mee zitten.

RS: Ja, dat is misschien ook lastig inderdaad.

Zorginstelling L: Ja en wat je dan wel ziet is dat mensen zich langzaamaan wel bewust worden ervan.. Het sijpelt wel maar het is niet dat ze zeggen van hee en nu gaan we het zo doen.

RS: Nee, want zijn er bijvoorbeeld al maatregelen voor medewerkers als ze zich er niet aan houden? Als ze bijvoorbeeld dingen niet melden?

Zorginstelling L: Maatregelen worden pas genomen als ze zich niet houden aan de gedragscode, die hebben we ook opgesteld voor informatiebeveiliging. Er is nu één incident geweest waarbij een medewerker een device had waarop ook patiëntgegevens stonden wat niet mocht en daar zijn wel maatregelen voor uitgezet.

RS: Ja, dus er zijn wel gedragsregels opgesteld voor informatiebeveiliging. En hoe kunnen die medewerkers die gedragsregels tot zich nemen?

Zorginstelling L: We hebben alle documentatie op het gebied van informatiebeveiliging gelinkt aan het kwaliteitsmanagementsysteem. En voor het kwaliteitsmanagementsysteem moet je al je beleidsafspraken op papier hebben staan, zodat mensen dat kunnen vinden en kunnen zien wat wij daar als instelling over afgesproken hebben. En we hebben daar een kwaliteitshandboek voor en die is opgedeeld in verschillende domeinen: zorg, organisatie, personeel, facilitair en kwaliteit en als ze dan naar de boomstructuur gaan dan kunnen ze bij facilitair zien hee informatiebeveiliging, daar kunnen ze alle documenten vinden die relevant zijn voor ze en dat kunnen ze gewoon lezen. En die gedragscodes staan bijvoorbeeld onder personeel en daar staan alle personeelsbeleidsvraagstukken in en ook de gedragscodes die ze daar kunnen vinden.

RS: Is dat dan hetzelfde als het intranet?

Zorginstelling L: Ja, dat is hetzelfde. Dat is een onderdeel van intranet. Dus als ze intranet opstarten dan kunnen ze daar gemakkelijk naar toe om documenten te vinden.

RS: En als je dan kijkt we hebben nu eigenlijk een soort tussenperiode: de Meldplicht Datalekken die is ingevoerd en straks gaan we naar de Europese Verordening toe die is natuurlijk al van kracht, maar straks in 2018 wordt die ook echt gehandhaafd. In hoeverre denk je dat jullie tegen die tijd voorbereid gaan zijn?

Zorginstelling L: Nou het is de bedoeling om begin 2017 op te gaan voor certificering en ik vrees dat we dat niet gaan halen.

RS: En dan bedoel je dat je dan een soort controle wilt laten doen?

Zorginstelling L: Ja, voor HKZ hebben we jaarlijkse audits die uitgevoerd moeten worden door een externe decaan en zij zouden voor ons ook de NEN-7510 gaan auditen, waardoor wij ook op dat gebied gecertificeerd zouden zijn. En ik was eigenlijk ermee bezig om dat voor januari te gaan inplannen, maar dat gaan we niet halen. We moeten nog zoveel voor awareness voorbereiden en uitrollen, dat gaat hem niet worden. Dus nu zijn er plannen om het misschien voor de zomer nog te doen en desnoods is het maar een nulmeting. Nou trouwens die nulmeting hebben we al gehad. Maar dan een eerste audit om te kijken van voldoen we nou eraan of niet en vandaaruit gaan we dan vervolgens bepalen hoe we verder gaan.

RS: Ja want er is dus wel een nulmeting gedaan.

Zorginstelling L: Er heeft wel een nulmeting plaatsgevonden ja.

RS: En wat kwamen daar voor belangrijke punten uit?

Zorginstelling L: Zij hebben eigenlijk geconstateerd dat we goed op weg zijn. Er waren een aantal aandachtspunten als het gaat om de toegang tot applicaties. Dan had ik een specifiek iets over authenticatie. En we moesten nog het een en ander doen op het gebied van die risicoanalyse dat mocht wat uitgebreider, dat hadden we vrij globaal en snel in elkaar gezet. Dus dat was één van de aandachtspunten en we moesten nog wat beter met onze leveranciers afspraken maken en niet alleen onze leveranciers, maar ook onze financierders aan wie wij gegevens verstrekken dat zij zich ook bewust zijn van de verantwoordelijkheid die zij hebben als wij gegevens uitwisselen. Dat zijn de belangrijkste punten geweest. En dat zijn allemaal punten die we nu hebben opgepakt en die risicoanalyse die hebben we nu gedaan dat is nu af. En die awareness dat is eigenlijk de volgende stap die we nu willen gaan zetten.

RS: Ja, precies. Want door wie werd die nulmeting dan gedaan?

Zorginstelling L: Dat is ook een extern bedrijf die daarvoor is ingehuurd.

RS: Oké, dus dan is nu eigenlijk die stap om met awareness aan de slag te gaan.

Zorginstelling L: Ja, en als je dat hebt gedaan dan kun je zeggen we gaan voor de zomer op voor certificering en dan is het gewoon rond.

RS: En hoe kijk je bijvoorbeeld tegen de rol aan van de Autoriteit Persoonsgegevens? Heb je informatie van hen ontvangen bijvoorbeeld?

Zorginstelling L: Nee, eigenlijk sinds die hele functie in het leven is geroepen, die functie voor functionaris voor de gegevensbescherming, je krijgt een brief dat het moet. Ik mis dan soms een verdieping daarvan. En dan word ik dat, maar dan moet ik me ook verdiepen in al die materie en wat er precies speelt. Ik bedoel ik wil het wel serieus nemen. En dan mis ik dat van oké we moeten aan een bepaalde eis voldoen, maar ik moet vervolgens wel zelf gaan zoeken wat ik moet doen om daar te komen zeg maar. En ik denk dat heel veel instellingen dat hebben dat ze daarmee zelf aan de slag gaan en nu later. Twee jaar later bijna starten ze een awarenesscampagne en dan denk ik ja jongens dat hadden we veel eerder kunnen bedenken met elkaar, dat hadden we gewoon met elkaar kunnen neerzetten en nu zijn we allemaal individueel bezig ermee.

RS: Ja, dat is ook de reden dat wij dit onderzoek zijn gestart natuurlijk. Kunnen we niet iets algemeens opstellen voor de zorgsector dat ze handvaten geeft om deze wet in de praktijk vorm te geven. Nou ik heb in ieder geval voldoende informatie voor mijn onderzoek. Ik weet niet of jij nog vragen hebt.

Zorginstelling L: Nee, ik heb verder geen vragen.

Nagesprek

Bijlage 6 Categorisatie interviews

6.1 Categorisatie interview zorginstelling A

Achtergrond van de Functionaris voor de Gegevensbescherming

A: 'Ik ben twee jaar geleden begonnen bij zorginstelling A en heb daar ook mijn afstudeeronderzoek gedaan. En toen is de zorginstelling begonnen met een impact en risicoanalyse in het kader van privacy omdat de Algemene Verordening Gegevensbescherming er aan zat te komen vanuit Europa die nu van kracht is vanaf mei. En op dat moment ben ik eigenlijk begonnen als jurist in het project dat die analyse ging doen en op dat moment was er al een functionaris gegevensbescherming werkzaam parttime. Toen bleek uit de analyse dat er toch wel wat werk aan de winkel was om te gaan voldoen aan de nieuwe AVG en toen hebben ze mij gevraagd eigenlijk of ik ook die functie wilde gaan doen, dus eigenlijk zodoende, omdat er gewoon de noodzaak was. Er moet wat gebeuren: de 24-uurscapaciteit die er was, was toch wel wat weinig, dus ben ik er bijgekomen voor 24 uur. Dus 48 uur FG'.

A: 'Ik ben FG met een juridische achtergrond en mijn collega had dat niet, dus dat was ook wel een pré dat ze mij graag wilden'.

A: 'Het is wel functionaris voor de gegevensbescherming dat is een wettelijk vastgelegde functie. Privacy Officer is dat niet. Ik heb zeg maar ontslagbescherming en ik moet onafhankelijk zijn en bepaalde taken zijn ook wettelijk vastgelegd zoals toezicht houden. Privacy officer is dat officieel niet'.

A volgt de leergang FG voor twee jaar.

Verhouding tussen privacy en de bescherming van persoonsgegevens

A: 'Ja, dat kan ik wel uitleggen. Je hebt het grondrecht, artikel 10 mocht je het willen opzoeken is jouw grondrecht op de bescherming van jouw persoonlijke levenssfeer dat betekent dat jij in je huis niet mag worden afgeluisterd, maar ook recht op lichamelijke integriteit, dat niemand zomaar aan je mag zitten. Dat is heel breed gezien jouw recht op privacy. Je mag gewoon in je eigen huis doen wat je wilt, niemand mag je zien, je mag niet worden afgeluisterd of gefilmd. Als je daarop inzoomt op dat hele grote brede privacy dan heb je natuurlijk ook een stukje persoonsgegevens: jij geeft persoonsgegevens aan Facebook of aan Gmail of aan waar je werkt, die verwerkt jouw persoonsgegevens. Die persoonsgegevens moeten ook worden beschermd en daar gaat eigenlijk de Wet Bescherming Persoonsgegevens over, de AVG, wat ik al noemde, dus eigenlijk moet je dat zien als een onderdeel van het hele grote recht op de bescherming van jouw persoonlijke levenssfeer'.

Belegging van de functie in de organisatie

A: 'Nee, we hebben geen afdeling. We hebben wel sinds ik ben aangenomen een privacywerkgroep opgetuigd. Dat is een kleine groep mensen waaronder dus twee FG's maar ook de informatiebeveiliger. Daar zitten nog twee juristen bij die voor een paar uur per week ondersteuning bieden en we hebben op dit moment nog een communicatiemedewerker, dat is ook tijdelijk. Dat clubje is de privacywerkgroep en daar kunnen mensen terecht voor advies en wij regelen daar zoveel mogelijk in. En die privacywerkgroep hebben we gepositioneerd onder juridische zaken, want het gaat om wetgeving, omdat dat de meest makkelijke manier is of neutrale plek is om deze werkgroep in te zetten. We hebben natuurlijk meerdere afdelingen, bijvoorbeeld medische zaken. Daar zou het natuurlijk onder kunnen, omdat je te maken hebt met patiëntgegevens, maar dan vergeet je eigenlijk weer de medewerkersgegevens, dus dat is dan weer niet helemaal overkoepelend. Dus dit was de meest logische plek'.

A: 'Die privacywerkgroep valt weer onder de staf. En staf is eigenlijk alle ondersteuning binnen het proces; personeelszaken, relaties alles zit daarin'.

A: 'Als we iets met communicatie willen, dan moeten we de afdeling communicatie ook inschakelen bijvoorbeeld. Daar hebben we dan automatisch contact mee en we hebben ook een lijn met de Raad van Bestuur. En wij leveren ook wel rapporten op, zeker naar aanleiding van datalekken, rapportage elke drie maanden'.

Samenwerking met communicatieafdeling

De verantwoordelijkheid voor het opstellen van communicatiebeleid ligt bij de afdeling communicatie en het communicatiebeleid wordt van daaruit geregeld. A: 'Uhm nee dat ligt dan bij de verantwoordelijke afdeling, maar wij kunnen daar wel in ondersteunen en aangeven wat daar nodig voor is en advies geven van waar iets moet staan bijvoorbeeld'.

A: 'Als er echt communicatiebeleid moet komen of dat er bepalingen moeten worden opgenomen extra vanuit die verordening, de AVG, dan is het aan het hoofd van die afdeling om onze input mee te nemen. Wij zijn niet verantwoordelijk, zeg maar'.
Over de uitvoering van het beleid zegt A: 'In principe moet dat dan via communicatie lopen of via een andere afdeling. We hebben ook beleid P&O bijvoorbeeld dat aangepast moet worden en dan moet die directeur daar ook voor zorgen. Het is wel zo dat ik als FG daarop moet toezien. Ik kan wel op een gegeven moment contact opnemen en eens vragen hoe het ermee staat, dingen controleren'.

Bekendheid met 'ZEKER' campagne
A is niet bekend met 'ZEKER' campagne van de NVZ.

Communicatie-inzet informatiebeveiligingsbeleid
A: 'Wat heel leuk is om ook nog te vertellen. Dat hebben dan trainees gedaan die wij ook bij de privacywerkgroep hadden. Die hebben belevingsonderzoek gedaan binnen de organisatie. Er hebben een paar stagiaires meegelopen in het primair proces met verpleegkundigen. Kijken: wat doen ze eigenlijk en een beetje het gesprek aangaan: laat maar zien wat je doet en wat kom je nu tegen als je denkt aan privacy, waar denk je dan aan? Wat voor dilemma's heb je dan in je werk? Want we willen ook wel graag dat het werkbaar blijft. Om zo mensen daarover na te laten denken. Niet alleen in de zorg, maar ook logistiek. Op alle soorten. Dat is wel heel leuk en daar hebben we ook wel wat ambassadeurs aan over gehouden, mensen die echt wel enthousiast zijn'.
A: 'En dat belevingsonderzoek is afgerond en daarna heeft de trainee nog klinische lessen gegeven en nog wat meer informatie over wat betekent dat nu allemaal en zo gaan we een beetje de organisatie wel door. En nu ook op andere plekken, want we hebben ons eerst gericht op het primair proces dus de zorg zeg maar. En nu gaan we ook kijken naar onze andere domeinen, zoals bedrijfsvoering waar de medewerkersgegevens liggen, maar ook onderzoek en onderwijs, ook een belangrijke. Maar echt evalueren, nee'.
A: 'Ja, wat we ook nog doen is we hebben elk jaar de dag van de patiëntveiligheid. En dan heb je allemaal standjes die allemaal met patiëntveiligheid te maken hebben en dan hebben wij ook een stand. En dan brengen we bijvoorbeeld die datalekken weer onder de aandacht'.
A: 'Het is heel groot, een soort van dorp met straten daarbinnen en in de grote straat is het dan met allemaal kraampjes, dat wordt groots aangekondigd van tevoren van de dag van de patiëntveiligheid kom allemaal kijken. Nou daar staan dan kraampjes. En we hebben ook vaak wel een bijeenkomst voor medewerkers. Vorig jaar hadden we iemand die ging vertellen over wat kan identiteitsfraude allemaal wat kan ermee gebeuren hoe erg is dat en iedereen schrikt zich dan rot natuurlijk. En we hebben er weer één in november, dan hebben we een hacker die gaat laten zien hoe en wat we allemaal een beetje aan het lekken zijn. Om ook, ja de bewustwording vooral dus weer te stimuleren zeg maar'.

Lastige groepen om te bereiken
Artsen als lastige groep. A: 'Ja, dat klopt wel. Dat is ook wel een lastige groep. Ja we nemen ze natuurlijk mee in de algemene campagnes. We hebben in ieder geval nog een student onderzoek laten doen binnen die groep naar hun intrinsieke motivatie om te voldoen aan dit soort wettelijke dingen. Even denken'.
A: 'Er is wel intrinsieke motivatie om het geheim te houden, want dat hoort bij hun beroep. Maar meer intrinsiek dan vanuit dat ze weten hoe het werkt in de wet, zeg maar'.

Thema in beeld bij bestuur
Op de vraag of ideeën binnen het thema privacy vaak door hen bedacht worden of vanuit de Raad van Bestuur en of zij dit thema een beetje goed in beeld hebben antwoordt A: 'Uhm, nee wij initiëren dit zeg maar, maar die brieven die wij de organisatie sturen, die gaan wel langs de Raad van Bestuur en ook onze rapportages datalekken.

Prioriteit van privacy in organisatie
En de Raad van Bestuur heeft natuurlijk wel ingestemd met het oprichten van de privacywerkgroep en met het aannemen van mij als extra functionaris van de gegevensbescherming, dus in die zin is er wel enigszins bewustzijn. Voor mijn gevoel kan het altijd meer'.

A: 'Ze hebben natuurlijk allemaal hun eigen portefeuille ook, dus er is één die dat in zijn portefeuille heeft en dat op zich ook wel belangrijk vindt, de anderen hebben daar iets minder feeling mee. Je hebt sowieso met zoveel mensen te maken, de één vindt het heel belangrijk, de ander vindt het irritante onzin'.
Zorginstelling A: 'Nee, volgens mij dit weet ik niet precies, volgens mij krijgt de privacywerkgroep wel een bepaald budget'.
Zorginstelling A: 'Ja, en dat moet zo min mogelijk. Het is volgens mij vooral budget voor de medewerkers. En extra we proberen heel veel dingen toch wel in de lijn te beleggen, omdat daar ook de verantwoordelijkheid ligt'.

Risico's in beeld bij bestuur
Op de vraag of de Raad van Bestuur zicht heeft op het risico van een datalek antwoordt A: 'Ja, dat hoop ik, maar dat weet ik niet zo goed of ze dat hebben. Sowieso zit er voor artsen nog een specifiek risico dat ze hun geheimhouding kunnen breken en dat ze dan voor een tuchtrechter worden gedaagd. En persoonlijk aansprakelijk worden gesteld, maar goed datalekken algemeen: je meldt het bijvoorbeeld niet, je komt toch in het nieuws of je neemt niet genoeg beveiligingsmaatregelen. Daar kun je ook vrij hoge boetes voor krijgen. Wij geven dat natuurlijk wel aan'.
A weet niet welke risico's een rol spelen bij de Raad van Bestuur: 'Nee, dat weet ik niet. Ik sta dan toch iets te ver van de Raad van Bestuur af om dat te weten hoe zij ernaar kijken, dat weet ik eigenlijk ook niet zo goed. Het belang wordt wel erkend, maar hoe ze er precies naar kijken dat durf ik niet te zeggen'.

Bijdrage van communicatie om risico's in te perken
A: 'Heel veel. Het grootste probleem met datalekken is het menselijk handelen, dus daar heb je het meest de medewerker gewoon bij nodig en die moet bewustzijn van wat ie doet, wil hij ook iets kunnen doen. Als je niet weet wat je aan het doen bent of als je onbewust gegevens aan het lekken bent of er gewoon slordig mee omgaat en bewust je computer niet afsluit of een scherm open laat staan in een vergaderruimte, waar dan nog patiëntendossiers openstaan terwijl de volgende club binnenkomt. Ja, als mensen daar niet bewust van zijn dan kun je daar ook heel weinig mee. Mensen bewustmaken, dus we zijn heel erg bezig met dat bewustzijn. En ook die datalekken helpen, want dat koppel je natuurlijk terug aan die afdeling: hee dit gebeurde er. Oh chips, nee dat mag natuurlijk niet en oh wat vervelend en daar gaan we meteen aan werken. Vaak wordt er dan in teamoverleg ook weer aandacht aan besteed dat er extra weer op gelet moet worden'.

Veranderingen in organisatie sinds Meldplicht Datalekken
A: 'Ja, voor 1 januari heb ik het proces al opgesteld en de communicatie ook gestart en ook aangegeven dat we nog een periode wilden oefenen als het ware. Vanaf oktober: begin maar met melden ook al is het nog niet officieel, dus we hebben eigenlijk vanaf oktober al meldingen gekregen, dat wordt wel meer'.
A: 'Ja, want we moeten natuurlijk zelf ook leren wat je dan voor dingen krijgt en hoe je dan een melding plaatst'

Meldingen
A: 'Nou dat wisselt heel erg, ongeveer vier per week. Maar dat kunnen soms dus vier op een dag zijn en soms ook in een week één'.
A: 'Ja, dat houden we bij, al die meldingen staan in het register'.

Procedure Meldplicht Datalekken
A: 'Nee, we hebben voor datalekken één werkproces gewoon ingericht eigenlijk voor alle medewerkers. Daarvoor hebben wij een telefoonnummer eigenlijk, we hadden al een telefoonnummer dat was de ICT-helplijn. Als jij bijvoorbeeld in de knoei komt met je computer, die doet het niet meer. Die hebben we gevraagd of ze ook de meldlijn willen zijn voor datalekken, bijvoorbeeld als jij in de trein iets verliest dan kan je ook bellen, ook als je dus niet op het werk zit. En ze kunnen meteen daar blokkeren op die afdeling. Daarom hebben we daarvoor gekozen. En dat hebben we breed gecommuniceerd: 'heb je een datalek, bel dit telefoonnummer''.
A: 'De ICT-medewerker die aan de telefoon zit die heeft van ons een vragenlijst gekregen van wat ze moeten uitvragen en daar vullen ze de antwoorden in en dat sturen ze naar ons toe. Wij doen de beoordeling en dat komt dan naar ons toe. Dan pakken wij het op. Wij doen de beoordeling, de FG's dan, of het ook bij de

autoriteit persoonsgegevens gemeld moet worden bijvoorbeeld. En of er maatregelen genomen moeten worden om het in de toekomst weer te voorkomen'.
Niet alleen naar zorgmedewerkers gegaan, maar naar alle medewerkers. A: 'Nee, naar alle medewerkers'.
A: 'We hebben voor extern nog niet een datalekportaal maar op zich willen we dat wel, dus we zijn daar wel mee bezig. Omdat bijvoorbeeld mensen ook wel eens een verkeerde brief krijgen, met bijvoorbeeld patiëntgegevens daarop van een ander. Dus dat is vrij vreselijk natuurlijk. En meestal komt dat wel bij ons binnen via de afdeling waar diegene onder behandeling is of dan belt die afdeling zeg maar ons nummer, maar eigenlijk willen we ook gewoon dat die mensen rechtstreeks iets kunnen melden. Nou hebben we wel een algemene plek: we hebben op onze website natuurlijk gewoon contact, maar we hebben ook meld het ons of bel ons knop waar mensen eigenlijk alle opmerkingen of feedback over alles wat ze maar kwijt willen over de instelling kwijt kunnen'.
A: 'Ja dat is dus heel algemeen. Dat komt terecht bij baliemedewerkers'.
A: 'Nee, dat hebben we dus nog niet, maar we hebben die behoefte op zich wel. Maar dat is de volgende stap'.
Op de vraag hoe het zit met de weekenden antwoordt A: 'Nou dat is nog lastig. We hebben daar eigenlijk te weinig capaciteit voor als FG. We hebben het wel zo gedaan dat de helplijn 24 uur bereikbaar is, dus als er echt iets ergs is, dan kan de meldlijn gebeld worden. Dan wordt het opgepakt. Stel er moet iets worden geblokkeerd, dan kan dat ook meteen worden gedaan en dan in principe is het wel zo dat de directeuren weekenddienst hebben, dan hoop ik dat er een directeur gebeld wordt, maar dat is nog niet helemaal officieel. Ik heb dat nog niet helemaal rondgekregen'.
A: 'We hebben dat nog niet goed voor elkaar gekregen om dat echt vast te leggen, omdat de directeuren daar ook niet altijd zin in hebben. En wij ook eigenlijk te weinig uren hebben om dat te kunnen'.
A: 'Nee, we kunnen geen 24-uursdiensten draaien dat mag ook niet verwacht worden met ons aantal uren, dat is heel simpel. Dus we halen het niet altijd. En ja wat vrijdag binnenkomt dat pakken we maandag weer op in principe. Dan ben je nog wel net op tijd, maar daar kan nog wel wat verbeteren'.
A: Je hebt van de Autoriteit Persoonsgegevens natuurlijk ook een meldformulier op internet en daar vul ik het op in. De meldingen doe ik en mijn collega FG.
A: 'Nou ja, ik bel vaak nog wel even terug naar diegene, want heb vaak nog wel wat extra informatie nodig, zoals wat er nou precies gebeurd is'.
A: 'Ja, vaak informeer ik de melder wel of ik het meld. En ook vaak de leidinggevende van de afdeling, hee dit is een datalek geweest, die ik ook heb gemeld bij de Autoriteit Persoonsgegevens, maar wat daar gebeurt daar heb ik geen zicht op he. Ik stuur het weg en dat is het'.

Communicatie-inzet naar aanleiding van Meldplicht Datalekken
A: 'Dat hebben we gedaan met een brief, dat is dan van de Raad van Bestuur, dat is een brief die gaat dan de hele organisatie door. En we hebben een intranet daar heeft het opgestaan. Daarin hebben we ook gecommuniceerd. Onze eigen intranetpagina, waar we ook informatie hebben en vragen van: wat is nu een datalek en wanneer moet je dan bellen en dat soort dingen. We hebben nog een flyer, ja we hebben nog wel wat flyers gemaakt. Ik heb nog wel wat meegenomen'.
A: 'Daar hebben we in die zin wel aandacht aan besteed. En we hebben ook, ja dan heb ik hier niet echt een goed voorbeeld van maar we hebben dergelijke dingen ook wel gewoon opgehangen: 'Datalek: bel'. We hebben ook wel op bepaalde afdelingen presentaties gegeven'.
A: 'We zijn wel bij verpleegkundigen overleg geweest bijvoorbeeld. Ja, beetje wel echt van die zorgafdelingen. Ik weet niet precies meer welke allemaal. Vaak wel een beetje op verzoek ook hoor, zo van: nou we willen nog wel wat extra informatie, we hebben die brief gelezen maar we snappen het nog niet helemaal'.
A: 'De presentaties zijn vanuit de privacywerkgroep verzorgd. En ook dit soort communicatiedingetjes (laat campagnetitel: 'Wat zou jij doen?' zien). Dit is bijvoorbeeld een campagne geweest voor de datalekken. Dit werd dan opengesneden met wat zou jij doen en daarachter stond dan een situatie beschreven. Bijvoorbeeld: Nou er ligt een dossier op de balie, wat zou jij doen? Om een beetje mensen te prikkelen zo van denk er eens over na'.
A: 'Ja en dit verspreiden we dan over het hele ziekenhuis'.
A: 'Ja, dan zie je dat en dan kijk je onder het flapje. De situatie staat onder het flapje met bovenop de vraag, wat zou je dan doen?'
A: 'Nee, nee dat moet je zelf bedenken. En die kwam op een gegeven moment op intranet. En dit heb ik zelf getekend ook toevallig'.

A: 'Meer dat we mensen wilden informeren van nou wat hebben we nu allemaal hoe kun je dat voorkomen met de informatie waar je dat moet melden'.
Onderzoeker vraagt of dat meer intern gebeurd is en niet in openbare ruimtes hing A antwoordt: 'Ja bij personeelskamers, bij printers. Nee, maar dit ook niet (bewustwordingscampagne) dit is ook bij personeelskamers, dit is voor medewerkers bedoeld natuurlijk niet voor patiënten'.
A: 'Bewustwording ook van goh wat gebeurt er nou en hoe kan je dat voorkomen. Om mensen weer aan het denken te zetten van goh oh dat is inderdaad wel herkenbaar. Of oja hier kan ik nog wel wat beter over nadenken of beter op letten'.
A: 'En deze hebben we ook nog. Dit is een checklist informatiebeveiliging en privacybescherming. En die was er al voor informatiebeveiliging, maar die hebben we dus uitgebreid met privacydingen en ook met de Meldplicht Datalekken'.
A: 'Ja, vooral. Ja, meldt mijn datalek staat hier. En nummers voor waar je dan heen moet bellen'.
A: 'Nee, maar ja dit is wel van de zorginstelling specifiek natuurlijk met ook onze interne telefoonnummers'.
A: 'Ja hier staan ook dingen in als: log je computer uit als je even naar het toilet gaat of als je even wegloopt. Dat je het niet open laat staan'.

Rol van de Autoriteit Persoonsgegevens
A: 'Ja vooral als externe toezichthouder'.
A: 'Nee, nee. Ze zitten wel op afstand zeg maar'.
A: 'Ja, maar ik weet dat zij daar geen antwoord op gaan geven, want ze willen heel erg de toezichthouder zijn en geen advies geven of ergens op in gaan'.
A: 'In mijn ervaring vind ik ze niet heel benaderbaar en ook als FG van een organisatie ook niet uitnodigend, want het is een toezichthouder, dus als je daar je vraag gaat stellen, krijg je misschien ook wel weer op je dak'.

Voorbereidingen op de AVG
A: 'Jij bedoelt de AVG? Die is 25 mei 2016 is die van kracht geworden, alleen twee jaar krijgen organisaties de tijd om eraan te gaan voldoen en dan in mei 2018 kan de Autoriteit Persoonsgegevens ook gaan handhaven. Dus vanaf dat moment kan de autoriteit ook boetes uit gaan delen binnen deze wet. Maar hij geldt nu al, dus je moet er al wel aan voldoen'.
Zorginstelling A: 'Ja, dat klopt maar dat is geregeld vanuit de Wet Meldplicht Datalekken, daar is de boetebevoegdheid groter gemaakt. Niet alleen voor datalekken, maar ook voor andere bepalingen. Dat is een bepaald bedrag, een bepaalde grens en de AVG heeft weer een andere grens en die is handhaafbaar vanaf 2018 en daarin staat bijvoorbeeld dat je documentatieplicht hebt, dat je daaraan moet voldoen, dus de organisaties moeten er nu aan gaan voldoen, maar over twee jaar pas kunnen ze daar een boete voor krijgen als ze dat dan nog niet op orde hebben'.
A: 'Ja, een overgangstermijn in feite'.
A: 'Wij doen hard ons best om daar klaar voor te zijn. Nee, dat is moeilijk te zeggen. Het is niet op één dag geregeld'.

6.2 Categorisatie interview Zorginstelling B

Achtergrond van de Functionaris voor de Gegevensbescherming
B: 'Maar ja hoe is dat gekomen, ja, dat is bijna een toevalsverhaal zeg maar. Op een gegeven moment ben ik gevraagd door de organisatie om risicomanager te worden en toen speelde het al dat het verplicht zou gaan worden dat er een functionaris gegevensbescherming zou komen en toen is ja hoe moet ik dat nou zeggen dat daarin gezet zeg maar in de functie van risicomanager'.
Aantal uur per week met de functie bezig: B: 'Ja, dat vind ik heel erg lastig. De ene week veel meer dan de andere. Maar ook weer niet zo heel erg veel, want dat moet ik er wel bij zeggen. Kijk ik ben een functionaris gegevensbescherming, maar als je kijkt naar de competenties zeg maar, dan zou dat toch iemand moeten zijn met een uitgebreide wetskennis en nou weet ik ondertussen uit ervaring een hele hoop, maar ik heb daar geen opleiding voor. Maar daar spar ik dan heel veel mee met de jurist van het ziekenhuis, de secretaris Raad van Bestuur, dus in die zin doen we het ook wel een beetje samen zeg maar'.
B: 'Als het echt over wetskennis gaat of dat soort dingen dan doet hij het met name en de meer operationele dingen die doe ik dan'.
B: 'Dus zo hebben we het een beetje verdeeld en ja hoe lang zal ik daar mee bezig zijn drie vier uur in de week, zoiets, een dagdeel denk ik gemiddeld'.

Belegging van de functie in de organisatie
B: 'Ik val rechtstreeks onder de Raad van Bestuur'.
B: 'Ik heb met de beide leden van de Raad van Bestuur, dat komt ook omdat ik een gedeelde functie heb zeg maar, maandelijks contact'.
Als het nodig is, worden voorvallen besproken met de Raad van Bestuur.

Thema in beeld bij bestuur
B: Ik denk dat, er zijn afgelopen jaar echt wel een paar rapporten geschreven zeg maar, ja, dan krijg je ook een beeld over hoe dat gaat in de organisatie en dat wij één van onze bestuurders werkt hier al twaalf jaar. Ja, ik denk wel dat die een beeld hebben.
Antwoord van B op de vraag of het niet bijvoorbeeld vanuit het bestuur komt van we moeten hier aandacht aan gaan besteden dit jaar: 'Nee, eigenlijk komt dat nauwelijks voor. Dat gaat andersom. Wij komen met voorstellen van hier zouden we aandacht aan moeten besteden en dat adviseer je dan en dan wordt dat door hen besloten. Zo gaat dat in de praktijk'.

Bewustzijn van medewerkers
Antwoord van B op de vraag of er al bewustzijn is bij medewerkers: 'Ja, steeds meer, maar medewerkers bereiken is best lastig. Wat ik net al zei en dat geldt voor dokters en voor medewerkers je hebt bij iedere communicatie een zender en een ontvanger en dat is lastig, want die ontvanger heb je in feite geen invloed op. Als je iets niet wil horen, dan hoor je niks'.

Risico's voor instelling van een datalek
B: 'Ja, ik denk dat dat bij ons is net zoals in ieder andere zorginstelling is. Er is heel veel aandacht voor natuurlijk de boetes die je kunt krijgen als je je datalekken niet meldt. Ik denk dat de risico's veel groter zijn op het vlak van imagoschade en dat soort dingen zeg maar. Dat zijn de belangrijkste risico's vind ik bij privacyschending'.

Bijdrage van communicatie om risico's in te perken
B: 'Nou kijk ik vind de belangrijkste rol van communicatie is echt mensen bewust maken van dat er regels zijn, maar mensen helpen zich daaraan te houden daar speelt communicatie niet zo'n rol'.
Onderzoeker vraagt of het daar gaat om het toezicht houden waarop B antwoordt**:** 'Ja, en ook duidelijk maken dat daar ook echt op toegezien wordt'.
B: **'**Mensen moeten merken dat dat gebeurt. Dat is hetzelfde als iedereen weet dat je niet door rood mag rijden maar toch gebeurt het veel. En daarmee wil ik niet zeggen dat mensen hier net zoveel de regels schenden als dat mensen op straat door rood rijden, maar het gebeurt wel. Dat kan ook niet anders. Ik bedoel er werken hier 2000 mensen'.

Wie stelt beleid op
Antwoord van B op de vraag of het bestuur ook het beleid opstelt: 'Ja, dat gaat in de praktijk niet zo hè. Kijk dat beleid dat wordt gemaakt door de mensen onder de Raad van Bestuur onder andere door mij. En zij uiteindelijk fiatteren dat. Zo gaat dat hè, wij doen een voorstel en natuurlijk kijken zij daar nog wel overheen van zijn we het daar helemaal mee eens, maar zij stellen het uiteindelijk vast zo gaat dat'.

Inrichting van informatiebeveiligingsbeleid
B: 'Wij hebben een privacybeleid. Dat heeft volgens mij ieder ziekenhuis wel. Maar we hebben ook procedures opgesteld rondom die datalekken. Daar is ook communicatie over geweest naar de organisatie toe. We hebben ook een loginbeleid opgesteld bijvoorbeeld van hoe doen we dat nou? Ja, ja, dus er is van alles.
B: 'Ja, ja zeker. Ja, daar is een procedure voor, want er is natuurlijk ook een procedure voor wat je wel en niet op lokale media mag opslaan, maar daar is ook beleid voor. Hoe ga je om met verwisselbare media. En het is ook zo dat in principe hier de usb-uitgangen niet werken, dus alleen op aanvraag en op argumentatie wordt die open gezet, maar daarmee maak je het niet waterproof. Nog steeds niet'.

Communicatie-inzet informatiebeveiligingsbeleid
B: 'Kijk in het beleid is het natuurlijk anders, want wat je mag en wat je kan zeg maar is afhankelijk van je functie. In de communicatie, kijk communicatie moet je in feite opsplitsen hè. Je doet een algemene

communicatie het huis in. We hebben hier zo'n weekblaadje en daar staat dan ook af en toe wat in over wat we constateren of waar we vinden dat aandacht aan besteed moet worden. Dat is geheel generiek'.
B: 'Maar wat ook gebeurt is dat je via de lijn communiceert, omdat je bepaalde groepen beter wilt bereiken zeg maar. Dan maak je onderscheid, dus dat is heel afhankelijk van waar je het over hebt'.

Veranderingen in organisatie sinds Meldplicht Datalekken
B: 'Ja, er wordt wel meer over gesproken, maar dat heeft niet alleen te maken met wat ik doe, maar dat heeft ook mee te maken dat wij in november vorig jaar het EPD in gebruik genomen hebben en vanaf dat moment zeg maar hebben wij nog strikter gekeken wie kan nu waarin en waarom en moet dat nu wel zo blijven. Daar zijn instellingen wel strenger in gemaakt dan dat ze waren en als dat soort dingen veranderen dan wordt er over gesproken. En dan weten mensen weer beter hoe de regels nou in mekaar zitten, want daar is natuurlijk toch nog wel discussie over, dat hou je altijd van is dit nou wel of niet toegestaan dat een medewerker dit wel of niet mag en behoort hij nou wel of niet bij het behandelteam. Daar is wel altijd discussie over, want je hebt natuurlijk ook wel een soort grijs gebied daartussen. Maar zo'n verandering zeg maar dat helpt wel in de bewustwording'.

Communicatie-acties naar aanleiding van Meldplicht Datalekken
B: 'Dat is geheel algemeen gegaan, dus iedereen dezelfde communicatie en dat is langs twee sporen gegaan. Dus dat is in het algemene nieuwsblaadje van het ziekenhuis gegaan uhm, maar ook via het MT de organisatie in dus via de lijn omdat een datalek in feite overal in de organisatie kan voorkomen. Dat wordt wel eens vergeten hè, want iedereen denkt altijd aan patiëntengegevens'.
B: 'Want iedereen als we het over privacy hebben, dan denkt iedereen alleen maar aan patiëntengegevens, maar medewerkersgegevens zijn natuurlijk net zo belangrijk. En dat vind ik dus de valkuil hè, want we zijn als zorg heel erg gefocust op de patiëntengegevens en aan de ene kant is dat goed, maar aan de andere kant is dat bijna een uitnodiging om de medewerkersgegevens te verwaarlozen'.
B: 'Nee, flyers niet. Er is aandacht besteed aan inderdaad de nieuwsbrief waarin ook verwezen werd naar ons intranet, waarin ook voorbeelden staan over waar je dan aan moet denken bij datalekken gewoon uit de dagelijkse praktijk in de zorg hè, als je op internet gaat zoeken vind je er genoeg. Dus op die manier besteed je daar aandacht aan, maar dan is, wat ik nou ga vertellen is meer verweven in mijn werk als risicomanager en ik ben vorig jaar begonnen met risicomanagement en dan moet je ook jezelf presenteren en duidelijk maken waarom gaat het nu als je het hebt over risico's en dan komt informatiebeveiliging ook aan bod en dat heb ik gepresenteerd in iedere sector in het ziekenhuis'.
Onderzoeker vraagt om verduidelijking: of het de bedoeling was de risico's onder de aandacht te brengen. B antwoordt**:** 'Ja, maar dan besteed je dus impliciet ook aandacht aan informatiebeveiliging. Dat is daar een onderdeel van natuurlijk, dat is één van de facetten van de risico's die er zijn. Dus op die manier ben ik ook in alle sectoren geweest en dus ook bij de staf'.
B: 'Ja, kijk er staat nog van alles op mijn lijstje, want we hebben altijd te weinig tijd zeg maar. Maar wat je natuurlijk graag zou willen is ook binnen een afdeling, gewoon eens casussen bespreken van wat kom je nu tegen en hoe zou je dat nu anders kunnen doen'.
Onderzoeker vraagt of er aandacht besteed wordt aan het meenemen van dingen naar huis of het vergeten uit te loggen van de computer. B antwoordt: 'Ja, zeker daar wordt zeker aandacht aan besteed. Maar ja dat blijft tegelijkertijd ook wel een lastige'.
B: 'Ja, je probeert mensen daar meer en meer bewust van te maken en dat lukt ook wel, maar daarmee maak je het niet waterproof zeg maar. Dat is ook bijna niet mogelijk denk ik'.
B: 'Ja wij hebben gecommuniceerd over die wet, dat die er is en hoe ze datalekken moeten melden en dat soort dingen dat gaat overigens op dezelfde manier als ieder ander veiligheidsincident, maar dat hebben we wel weer opnieuw gecommuniceerd ja'.

Vragen van medewerkers
Onderzoeker vraagt of B dan ook wel eens van afdelingen iets te horen krijgt als ze ergens tegen aan lopen en hoe die barrières dan worden opgepakt. B antwoordt: 'Daar ging net het gesprek over. Dat gaat dan heel expliciet ging over een OK die toegang wil hebben tot de radiologiebeelden en dan is de discussie is nou die OK-assistent onderdeel van het behandelteam van de patiënt. Dat is zeg maar de bepalende vraag of zo iemand dat mag, daar bij mag bij die beelden, dus heb je een doelbinding en daar kun je op allerlei manieren naar

kijken en dat was net heel erg aan de hand. Dat is best een ingewikkelde vraag ook nog waar we nog niet uit zijn zeg maar'.

Procedure Meldplicht Datalekken

B: 'Wat we gedaan hebben in onze VIM-applicatie, ik weet niet of je dat wat zegt? VIM is een systeem Veilig Incident Melden daarmee kun je dus meldingen maken over incidenten daar hebben wij een categorie gemaakt informatiebeveiliging en dan kunnen ze dat invullen dan krijg ik daar samen met de andere twee leden van de informatiebeveiligingscommissie een mail van. En daarop ga ik dus aan de slag van wat is er nou precies gebeurd en moet dit gemeld worden en hoe dichten we het lek en noem maar op, dus ja'.
Onderzoeker vraagt of de medewerker daarin ook wordt meegenomen. B antwoordt: 'Die krijgt terugrapportage en heel vaak, maar dat is niet altijd nodig, benader ik die dan ook van ja hoe zit dit en hoe zit dat'.
B: 'Die 72 uur als ik er ben is dat oplosbaar'.
B: 'Nee ik ben er in het weekend niet, maar daar is die 72 uur voor. Het zou eerst 48 uur worden, maar dan heb je in de weekenden een probleem, maar wij hebben het zo geregeld dat met ons drieën er is altijd iemand. Dus als ik vakantie neem dan neemt één van die andere twee dat over'.
Medewerkers weten dat er een meldpunt is en weten hoe ze incidenten moeten melden. B: 'B: Ja, dat moeten ze weten, want ze moeten ook andere incidenten daarop melden'.
B: 'Ja dat kan via intranet hè, kun je die melding doen'.
B is daarnaast ook telefonisch bereikbaar: zijn nummer staat gewoon op internet. Onderzoeker vraagt of er dan ook een extern meldpunt is. B antwoordt: 'Dat is hetzelfde meldpunt alleen vanuit extern kun je natuurlijk niet bij die VIM-applicatie, maar als je gaat kijken naar het internet dan staat ook bij privacy staat dat als ze daar klachten of vragen over hebben dat ze mij kunnen bellen'. Onderzoeker vraagt door of er dan ook rechts in de hoek staat bijvoorbeeld 'meld uw datalek'. B antwoordt: 'Ja, zo staat dat er bij ons niet. Maar wel als je privacy intypt op de zoeker dan kom je bij mij terecht'.
Onderzoeker vraagt of het ook mogelijk is om anoniem te melden. B antwoordt: 'Ik denk, maar dat weet ik niet zeker, dat je je naam niet perse in hoeft te vullen, maar ik heb het ook nog nooit meegemaakt dat er een naam niet bijstond zeg maar'.
B: 'Ja, zo gauw als er informatiebeveiligingsincidenten zijn, hebben wij daar zeg maar een commissietje voor die dat onderzoekt. Dan ben ik degene die dat praktisch onderzoekt en dan maak ik een rapport. Dat stuur ik naar die andere twee leden. Dat bespreken we dan eerst even samen en dat gaat altijd naar de Raad van Bestuur'.
Als er een melding wordt gedaan van een datalek of een mogelijk datalek dan gaat dit altijd eerst langs de Raad van Bestuur voordat bijvoorbeeld de Autoriteit Persoonsgegevens wordt ingelicht. De Raad van Bestuur kan uiteindelijk beslissen of zij de AP inlichten. De verantwoordelijkheid ligt dus bij de Raad van Bestuur. B: 'Ja, volgens mij is dat per definitie zo'. B: 'Ja, ja ik heb een onafhankelijke functie dat is zeker zo. Maar de Raad van Bestuur is ook hoofdelijk aansprakelijk op het moment dat het fout gaat. Dus vind ik het heel logisch dat zij degene zijn die daar het eindoordeel over vellen'.
B: 'Kijk als het een onderzoek is naar een datalek dan maken wij een rapportje hè in de praktijk is het dan meestal zo, ik maak het rapport en die anderen die lezen mee en geven op of aanmerkingen daarop en in dat rapport staat dan het advies voor de Raad van Bestuur; het wel of niet melden, de betrokkene melden dat staat daar'.
B: 'Dus wat we dan doen meestal is de betrokkene horen hè wat is nou jouw reden om dat wel te vinden of niet te vinden en dan bespreken we dat, bespreek ik dat meestal met de jurist en als we dat dan nog moeilijk vinden dan hebben we ook nog een autorisatiecommissie, dus dat is dan nog een wat groter verband waarin je dan discussieert'.

Beveiligingsmaatregelen

B: 'Ik vind dat enorm moeilijk. Hoe dicht je dat soort gaten nou af. En we hebben nog niet zo lang een incident daarmee gehad. Dat was een usb-stick die was vijf jaar geleden gemaakt en toen nog heel begrijpelijk want er moesten gegevens naar de zorgverzekeraar. Dat kon niet anders in die tijd als met die usb-stick. Maar zo'n usb-stick die ligt nog in zo'n la en op een gegeven moment zo'n la van zo'n ladeblok en die is stuk en die wordt afgevoerd en dan vinden we die usb terug. Nou gelukkig vinden wij hem op dit terrein nog terug, maar voor hetzelfde geld'.
Onderzoeker vraagt of dingen als een gestolen laptop geblokkeerd kunnen worden van afstand. B antwoordt: 'Als een laptop gestolen wordt kun je er niet bij, maar in principe is het zo dat als mensen in het

ziekenhuissysteem willen dan moeten zij hun account openen. En dat kunnen we stoppen. En er is een dienstdoende van de ICT, dus ja dat kan. Maar hebben mensen lokaal wat staan en het wordt gestolen, dan kun je niet verder. Daar kun je niet bij dat kun je niet blokkeren van afstand. Maar het beleid is dat ze dat niet mogen doen'.
Onderzoeker haalt voorbeeld aan van datalek Antoni van Leeuwenhoekziekenhuis. B zegt daarover: 'Ja, dat zijn van die voorbeelden waarvan iedereen weet dat dat niet mag, maar toch gebeurt het. En daar durf ik hier mijn hand ook niet voor in het vuur te steken. Er wordt genoeg over gecommuniceerd en mensen weten intussen wel dat dat niet mag'.

Voorbeeld van niet-officiële communicatiemethode die goed werkt
B: 'Maar wat ik bijvoorbeeld ook doe is één keer in de maand lees ik logins uit van ons EPD en dan ga ik gewoon gericht kijken van wie heeft er nu waar in gezeten en waarom en daar komen natuurlijk vragen uit voort en dat werkt heel erg goed'.
B: 'Ik kan alles zien wat medewerkers in de afgelopen tijd, wat iedereen doet in het EPD. In andere systemen is dat wat moeilijker, een aantal systemen kan dat wel, een aantal kan dat niet. Maar wat je dan doet is, om te beginnen kijk ik altijd, dan wordt het heel technisch hoor, maar als je in de EPD dan heb je vrij toegang tot een dossier als je daar een behandelrelatie mee hebt, dan wordt dat ook gelogd maar dan kun je er zomaar in. Op het moment dat je een dossier in wilt, waarvan niet in het EPD duidelijk is dat je daar een behandelrelatie mee hebt dan krijg je een pop-up van waarom wil je hierin? En dat noemen ze de break the glass methode. Daar staan een aantal voorkeuzes en de laatste is anders en dan moet je het zelf invullen hè als die keuze er niet in staat. Daar begin ik altijd mee om gewoon van een aantal weken te kijken, wie heeft de break the glass methode gebruikt en dan kijk je naar de redenen. Dan haal je er bijna altijd wel een paar uit waarvan je denkt ja wat staat hier nou eigenlijk want dan is het gewoon niet duidelijk dus dan krijgen mensen er een mail over van je hebt dat als reden opgegeven maar wat betekent dat nou?'
B: 'Maar het komt ook voor dat mensen daar opgeven van nou dat doe ik omdat ik een eerste consult wil afspreken en dan ga je kijken, maar kan je geen eerste consult vinden. Nou, daar krijgen mensen ook een mail over. Ik zie dat je daar de reden opgegeven hebt: eerste consult, maar ik zie hem niet, wat is er aan de hand? Of je hebt een collegiaal consult of nou noem maar op'.
B: 'En dat werkt heel erg goed, want dat is natuurlijk geen officiële communicatie, maar wat er dan gebeurt is dat mensen onderling gaan praten van 'hee ik krijg een mail en ik moet verantwoording afleggen waarom ik dit of dat doe' en dat spreekt zich heel snel rond'.
B: 'Ja, ik krijg nu zelfs soms mailtjes van mensen die zeggen ja ik ben in dat dossier geweest en daar en daarom dan weet je dat vast'.
B: 'Ja en dat is natuurlijk wat je wilt. Je wilt dat mensen erover na gaan denken van moet ik hier wel in?'
B: 'En ik ga in principe uit van goede bedoelingen van iedereen en toch is het zo dat mensen soms, ja om een onbenullige reden in een dossier gaan kijken. En ja dat moeten we ze gewoon afleren'.
B: 'Om je een voorbeeld te noemen, een recent voorbeeld. Krijg ik van iemand een mailtje, die voelde natuurlijk al wel dat dat niet deugde, maar die had een boek geleend van een patiënt en een beetje te lang in zijn bezit gehouden en die was dan in het EPD gaan kijken of die patiënt nog leefde, want die was ernstig ziek toen ze dat boek uitleende. Ja, ik snap het wel, maar het mag gewoon niet. Daar is het EPD niet voor bedoeld'.
B: 'Maar dat soort dingen die probeer je er natuurlijk uit te krijgen. Het is hartstikke goed bedoeld en dat geloof ik ook meteen, maar het mag gewoon niet. Dan moet je het op een andere manier oplossen. Nou dat soort dingen probeer je eruit te halen. En dan heb je natuurlijk ook en dat heb je in ieder ziekenhuis, dat je toch even gaat kijken waarom de buurvrouw in het ziekenhuis was. Ja, dat mag natuurlijk helemaal niet. Dan krijgen mensen ook echt een gesprek. Als je dat soort dingen signaleert van wat ben je nou aan het doen?'
Ze krijgen dan een gesprek met B en hun leidinggevende, omdat zulke dingen 'gewoon niet mogen'.
B: 'En je kunt het niet altijd achterhalen, want je bent natuurlijk wel gebonden, ook ik moet me aan de privacyregels houden en wat ik bijvoorbeeld niet mag en eigenlijk wel graag zou willen is gewoon postcodes vergelijken. Postcodes van medewerkers en patiënten. Maar dat mag niet, want je hebt doelbinding. Toch vind ik het wel jammer dat dat niet mag, want dan kun je veel gerichter gaan zoeken van wie doet er nou wat. Nu moet ik daar bij toeval achter komen. Maar dan kun je gerichter zoeken, maar dat soort dingen mag niet en daar hou ik me dan ook aan, maar ik vind het wel eens jammer'.
B: 'Ja, maar mensen doen het ook vaak omdat ze het toch wel eng vinden om het aan iemand gewoon te vragen van hoe is het nou. Maar ja het mag gewoon niet. En je moet het ook niet willen hè. Ik probeer mensen ook altijd uit te leggen privacy is één het mag gewoon niet dus je doet het niet. Maar daarnaast vind ik ook

oprecht je moet het niet willen weten. Als jij mijn buurvrouw bent, dan moet ik toch niet willen weten waarom jij in het ziekenhuis bent geweest. Dat moet ik aan jou vragen en als jij dat niet wil vertellen dan moet ik dat niet willen weten. Daardoor breng je jezelf ook in de problemen hè, want je krijgt hele rare verhoudingen daarmee. Ik werk natuurlijk al heel lang in een ziekenhuis en heb daar echt de raarste dingen van gezien. Daar moet je echt, daarmee breng je echt jezelf ook in de problemen. Even los nog van de privacy is het heel handig dat jij dingen weet van de ander waarvan de ander niet weet dat jij ze weet'.
Antwoord van B op vraag van onderzoeker dat er steeds meer medewerkers zijn die uit zichzelf komen: 'Ja en daar was dit en dit de reden van. En meestal is dat dan een reden die ook legitiem is hè, maar niet altijd en dan probeer je mensen daar ook wel duidelijk op te wijzen, waarom dat dan niet mag en wat ik dan natuurlijk ook wel doe daar heb ik wel een lijstje van zeg maar en dan toch nog een keer gericht kijken van hebben ze het niet toch nog gedaan daarna'.
B: 'Ja, kijk als je ze gewaarschuwd hebt dat het niet mag en ze doen het dan toch wordt het serieus'.
B: 'Ja, dat spreekt zich rond hè, dat past natuurlijk ook wel een beetje bij de omvang van deze instelling. Hier wordt natuurlijk toch wel een beetje gesproken van het dorp, zeg maar. Wij hebben natuurlijk niet een enorme instelling dus heel veel mensen kennen elkaar en dan werkt dat natuurlijk beter dan in een academische kliniek waar je mensen tegenkomt die je nog nooit gezien hebt'.
B: 'Ja, dit werkt. Dit werkt beter dan één keer in de week in zo'n blaadje wat zetten, want dat leest toch echt niet iedereen hoor'.

Lastige groepen om te bereiken
Voorbeeld wordt aangehaald van artsen als lastige groep door onderzoeker. B antwoordt: 'Uh, er wordt gecommuniceerd naar hen ook via het stafbestuur, dus zij worden ook gericht benaderd, maar bij alle communicatie is het zo dat je last hebt van een zender en een ontvanger, maar dat is niet alleen bij dokters zo'.
Onderzoeker vraagt of er ook presentaties gegeven worden op afdelingen. B Antwoordt: 'Uhm, dat gebeurt. Presentaties op afdelingen, maar artsen zijn geen onderdeel van de afdeling. Tenminste op de meeste plaatsen niet en op specifieke afdelingen wel natuurlijk, maar op de meeste plaatsen niet, dus die kun je op die manier niet bereiken'.
Onderzoeker vraagt hoe je ze dan wel kunt bereiken B: 'Via de staf. Zij hebben ook stafoverleg één keer in de zoveel tijd. Op die manier probeer je die dan te bereiken of via mailing, dat soort dingen'.

Motivatie om te gaan melden
B: 'Ja, maar kijk je kunt niet meer doen dan mensen erop wijzen dat het belangrijk is om te melden en waarom het belangrijk is. Over het algemeen is het toch gewoon zo dat medewerkers in de zorg het ook wel belangrijk vinden dat privacy bewaakt blijft dus ze hebben ook wel een interne motivatie, ja en er is dan die VIM-melding waarbij het juist nadrukkelijk bedoeld is om mensen zonder dat daar represailles tegenover staan ook kunnen melden. Ja veel meer kun je niet doen'.

De rol van de Autoriteit Persoonsgegevens
Onderzoeker vraagt of B ook informatie gekregen heeft van AP. B antwoordt: 'de algemene communicatie die iedere zorginstelling heeft gehad. Je krijgt ook gerichte communicatie. Ook via de NVZ'.
Onderzoeker vraagt hoe B tegen de rol aan kijkt van de Autoriteit Persoonsgegevens. B antwoordt: 'Tsja… Ik moet zeggen dat ik niet vind dat die heel proactief zijn'. Onderzoeker kan zich voorstellen dat je soms met vragen zit of je dan contact opneemt met de AP. B antwoordt: 'Ja dat kan hè. Er is een telefonisch spreekuur iedere dag. Ik heb wel eens met hen gepraat'. Onderzoeker vraagt of B dan ook antwoord heeft gekregen. B antwoordt: 'Ja, uiteindelijk wel, ja ik vind wel, ja je krijgt wel antwoord op je vragen, niet altijd een bevredigend antwoord maar goed dat ligt niet alleen aan hen maar ook aan mij denk ik, maar wat wel lastig is je belt dan naar zo'n telefonisch spreekuur dan heb je niet altijd degene ervoor die jouw antwoord kan geven, dus soms gaat er dan toch wel wat tijd overheen voor je antwoord hebt. Uiteindelijk krijg je het wel is mijn ervaring, maar soms duurt het wel te lang'.
Onderzoeker vraagt of de wetten duidelijk waren. B antwoordt: 'Niet altijd natuurlijk maar weet je we hebben hier een regionale privacycommissie waarbinnen we ook over dit soort dingen spreken. Ik zit in het netwerk informatiebeveiliging dus je krijgt ook via het netwerk krijg je informatie, dus uiteindelijk kom je daar wel uit'.
B: 'Iedereen is er bang van hè. Ja, en misschien wel terecht ik weet het niet kijk tot nu toe is er natuurlijk nog niets gebeurd en dat was natuurlijk ook wel de verwachting het was niet te verwachten dat per 1 januari meteen de boetes om de oren zouden vliegen'.

B: 'Het zou ook contraproductief zijn, want dan zouden mensen ook schroom gaan krijgen om dingen te melden, dus dat was ook niet te verwachten. Maar uiteindelijk zullen zij natuurlijk gaan handhaven en ook wel terecht, maar je zou een gemakkelijkere toegang tot hen moeten hebben en tot hun kennis moeten hebben. Maar ik denk dat wat jij zegt daar hebben zij uiteindelijk ook helemaal de capaciteit niet voor'.

Voorbereidingen op de AVG
B: 'Nog niet. Er zijn echt nog dingen die anders moeten en zoals ik al zei we zitten in zo'n regionale privacycommissie, dus dan ben je ook wel op zoek zeg maar om daar wat in de gezamenlijkheid aandacht aan te besteden om het wel op tijd op orde te krijgen'.
Onderzoeker vraagt of er een stappenplan is om daar op voorbereid te gaan zijn B antwoordt dat dat er nog niet is, maar dat dat er wel moet komen natuurlijk.
Op de vraag van de onderzoeker waardoor het denk je komt volgens B dat veel bedrijven nog geen plan hebben voor de AVG antwoordt B: 'Het duurt natuurlijk nog lang hè'.
B: 'Nou dat moet gaan komen, ja dat moet zeker gaan komen, maar zoals ik al zei proberen we het toch een beetje regionaal op te pakken zodat we niet allemaal zelf het wiel aan het uitvinden zijn'.
B: 'En de tijd ontbreekt soms ook hè'.
Onderzoeker geeft aan dat dat kan komen doordat het nog geen fulltime functie is. B antwoordt: 'Ja, maar dat gaat het in deze instelling ook niet worden. Dat is onbetaalbaar. Kijk dat is het lastige hè met een instelling van onze omgang. Je kunt niet voor al dit soort dingen iemand aanstellen, want dat is veel te duur'.

6.3 Categorisatie interview zorginstelling C

De functie van de Functionaris voor de Gegevensbescherming
C: 'Nou ik werk al sinds 2003 bij deze instelling. Ik ben begonnen bij een secretaressefunctie eerst bij de jeugd gezondheidszorg en in 2008 ben ik doorgestroomd naar de Raad van Bestuur. Eind vorig jaar kwam de functie functionaris gegevensbescherming op de borden hier en toen werd ik benaderd door onze bestuurder of ik daar interesse voor zou hebben. Daar heb ik even, nou ja best even over nagedacht, want het is natuurlijk een hele andere soortige functie en ik heb ook helemaal geen juridische achtergrond ik heb ook helemaal geen ICT-achtergrond dus ja, ik moest eigenlijk in het diepe gegooid worden. Ik ben uiteindelijk wel de selectieprocedure ingegaan en ben toen per 1 december aangesteld als FG-er. Ik doe de functie wel met ondersteuning van de informatiemanager, dus ik doe het niet helemaal alleen. Ik heb wel een onafhankelijke positie, maar op ICT-gebied word ik echt ondersteund door de informatiemanager en hij is ook vorig jaar al betrokken geweest bij onder andere de risico-inventarisatie. Dus hij is vanaf het begin af aan eigenlijk betrokken geweest bij het hele traject'.
C: 'Nee, ik werk 16 tot 24 uur, doe ik de functie en ik weet natuurlijk niet hoeveel uren de informatiemanager er exact aan besteed, maar het zal om en nabij in zijn totaliteit om een fulltime functie gaan. Ja, we zijn natuurlijk een zorginstelling dus we werken veel met gegevensverwerkingen, dus er komen ook veel vraagstukken naar voren en ik moet wel eerlijk zeggen dat ik een tijd in een overgangsfase heb gezeten. Mijn collega kreeg ook een andere functie hier intern en onze oude functie die werd niet gelijk naar behoren ingevuld dus we hebben een tijd met één been hier en één been daar, maar goed sinds 1 september is het echt goed gefaciliteerd en kan ik mij echt helemaal richten op deze functie'.

Belegging van de functie in de organisatie
C: 'Nee, nog niet. Wij zijn wel momenteel aan het kijken naar een andere organisatiestructuur waarbij mijn functie waarschijnlijk wordt ingedeeld bij afdeling beleid, zo'n functie komt er weer en ik denk ook dat de positie daar goed zit. Ik hang nu echt onder de Raad van
Bestuur en dan kom ik onder een concernmanager. Zo ziet het plaatje eruit, maar we hebben geen aparte afdeling privacy of security. We zijn ook maar met zijn tweeën'.

Prioriteit van privacy in de organisatie
C: 'Nou wij hebben zeg maar wel een stuurgroep, een stuurgroep informatiebeveiliging, daar zit de bestuurder ook bij, de informatiemanager en ik zitten daarbij. En we hebben een klankbordgroep die komen eens per kwartaal bij elkaar, de stuurgroep maandelijks en we hebben altijd maandelijks MT waar dit punt ook wel op de agenda staat. Dus het is in die zin wel geborgd overal, maar wij zitten momenteel best in een periode waar andere zaken ook hoge prioriteit hebben en dan merk je toch dat, tenminste dat idee heb ik, dat het bij

mensen is van oh heb je dat gezeur weer, moeten we dat ook weer gaan doen. Dus dat is best een beetje lastig'.
C: 'Ik denk, nee denk is niet het goede woord, ik vind dat het een hoge prioriteit heeft bij heel veel mensen, maar ik denk bij de medewerkers die echt zorg willen verlenen dat dat niet zo heel erg meespeelt'.
C: 'Dat die toch wat, ja of er niet bij stil staan of weet je vroeger deden we het ook zo dus waarom zouden we het nu niet zo doen, de verandering is dan heel lastig. Aan de andere kant denk ik ook dat je ook niet te gespannen ermee om moet gaan'.

Verhouding tussen privacy en de bescherming van persoonsgegevens
C: 'Ja, bij ons is dat allemaal één pot nat zeg maar'.
C: 'Ja, we hebben daar geen scheiding in. Nee, alles valt onder één en dezelfde noemer'.

Informatie over de instelling
Antwoord van C op vraag van de onderzoeker hoeveel mensen er werken: 'uhm, om en nabij de 2000'.
Antwoord van C op vraag van onderzoeker wat voor soort medewerkers toegang hebben tot patiëntgegevens: 'Nou die zijn allemaal wel, we werken met een ECD, die is nu de pilotfase voorbij, dus die zijn we nu gefaseerd aan het invoeren. Ja, hier op kantoor werken voornamelijk beleidsmedewerkers er zit een stuk huishoudelijke verzorging, maar dat zijn dan de managers, de planners, de reïntegratiespecialisten op kantoor en de uitvoerende medewerkers dat zijn onder andere de wijkverpleegkundigen, huishoudelijke hulpen, maar ook artsen van de JGZ, verpleegkundigen van de JGZ, we hebben een heel breed scala van mensen die daar werken en die zijn allemaal op basis van hun functie, hebben die autorisatie gekregen voor wij werken met ONS van NEDAP dat is een cliëntendossier, een systeem en die zijn op basis van hun functie zijn zij geautoriseerd en hebben zij toegang'.
Antwoord van C op vraag of de hoofden van de verschillende afdelingen wel in dit gebouw zitten: 'Ja, dat zit allemaal wel hier'.
Antwoord van C op vraag of medewerkers zoals wijkverpleegkundigen wel een vaste plek hebben of altijd dynamisch over de regio verdeeld zijn: 'Ja voornamelijk. Wij hadden voorheen altijd rayonkantoren, maar daar hebben we een heel aantal van afgesloten, dus de plekken worden steeds minder. Maar er zijn nog wel een aantal kantoren waar zij nog wel terecht kunnen, maar het meeste is dynamisch. Want als ze naar kantoor gaan mogen ze daar eigenlijk geen tijd voor schrijven, dus eigen tijd, dus het merendeel gaat inderdaad dynamisch'.

Wie stelt beleid op
Antwoord van C op vraag van onderzoeker of C degene is die ook het beleid opstelt rondom het thema privacy: 'Ja, in combinatie. Wij hadden geen Sec of privacybeleid, dus daar zijn we vorig jaar mee aan de gang gegaan. Daar heeft de informatiemanager als eerste het voortouw in genomen. Dus hij heeft het beleid geschreven, want hij is tevens MT-lid. Ik heb op basis daarvan een informatiebeveiligingsplan geschreven en een plan van aanpak Meldplicht Datalekken dus met die drie notities hebben we zeg maar één grote notitie gemaakt en die is begin van dit jaar ook in het MT vastgesteld en die wordt nu geïmplementeerd in de organisatie verder'.

Communicatie-inzet informatiebeveiligingsbeleid
C: 'Het wordt gepubliceerd op intranet. Er wordt ook aandacht gegeven dat het gepubliceerd is dat het er staat'.
C: 'Uhm, ja we hebben nu binnenkort hebben we een training privacy die wordt gegeven door een advocatenkantoor'.
C: 'Ja, nieuwsbrieven gaan maandelijks, die verstuur ik. Die gaan ook wel weer via het intranet, maar ook deels via de mail. Met het verzoek ook om die breder te verspreiden. We gaan binnenkort een enquête uitdoen, een enquête gebaseerd op de NEN7510 die willen we een beetje als nulmeting gaan gebruiken van hè hoe leeft het nou bij de mensen en die willen we ook uit gaan zetten onder een breed scala dus zowel op topniveau als ook op het niveau van de werkvloer, maar ook bij de huishoudelijk verzorgenden en dan willen we hem over een half jaar of negen maanden weer een keer herhalen van wat is nu: hè hoe staat het nu is er wat veranderd en waar hebben mensen behoefte aan? Hoe zouden zij informatie graag aangedragen krijgen?'
C: 'Ja, en wij zijn er als organisatie niet heel sterk in hoor om dingen te communiceren. Wij mogen bij onze communicatie, dat komt overal naar voren bij de medewerkersmonitor, communicatie komt altijd naar voren als toch een zwak punt'.

In eerste instantie is het zo dat het vanuit de top gaat. Het MT heeft die stukken vastgesteld, dan gaan die stukken via het betreffende MT-lid verder naar de divisie naar de leidinggevenden en de leidinggevenden die nemen dat dan weer mee in hun overleggen met de teams'.
Onderzoeker geeft aan dat je daarnaast natuurlijk het privacyreglement hebt en vraagt hoe dat wordt gecommuniceerd C antwoordt: 'Ja, dat kunnen mensen lezen op intranet, maar dat is niet actief. Ja, het staat daar'.
Onderzoeker vraagt hoe je er dan wel voor kan zorgen dat mensen dat gaan lezen C antwoordt: 'Ja, we willen het ook onderdeel gaan laten uitmaken van het functioneringsgesprek. Gewoon een agendapunt: het hoort erbij net zoals dat je een opleiding bespreekt tijdens je functioneringsgesprek. We willen het niet als wijzende vinger, maar gewoon van hoe ga je nou om met. Je krijgt het nooit waterdicht, want je kan mensen laten tekenen of je kan mensen een vinkje laten zetten, maar je kan nooit toetsen of je het nou daadwerkelijk hebt gelezen dat is heel moeilijk om een vinger op te krijgen. Ja, net zoals weet je melden mensen alles wel? Ja ze melden niet alles, dat weet ik zeker'.

Verschillende benaderingswijze voor verschillende groepen
C: 'Nee, daar zijn we aan het kijken.

Lastige groepen om te bereiken
C: 'Het wordt gepubliceerd op intranet. Er wordt ook aandacht gegeven dat het gepubliceerd is dat het er staat. Maar daar heeft niet iedereen toegang tot want niet alle medewerkers hier hebben een eigen account. Want ja de gewone verzorgende die hoeft eigenlijk niks met een mailadres van de instelling. Dus ook op basis van kosten hoor is er voor gekozen om die geen account meer te geven. Dus die bereik je dan ook niet, zij hebben ook geen werkoverleggen, komen nauwelijks meer op kantoor, dus ja dat is lastig. Dat is een lastige groep om te bereiken'.
Antwoord van C op de vraag van de onderzoeker of er ideeën zijn om die groep te bereiken: 'Uhm, ja we hebben nu binnenkort hebben we een training privacy die wordt gegeven door een advocatenkantoor. Daar zit ook de leidinggevende van de HV (Hoofd Verpleegkundigen) bij en zij communiceren ja, via ons medewerkersportaal, dus dan gaat het via die weg, hebben zij wel toegang'.
Antwoord van C op vraag of wijkverpleegkundigen online hun diensten kunnen zien: 'Ja, dat gaat via dat Ons'.
Antwoord van C op vraag of die mensen dan gewoon worden gebeld door de patiënten als er iets is: 'Ik weet niet of zij rechtstreeks benaderd kunnen worden, ze zullen het nummer in hun telefoon hebben en anders gaat het bij ons via de zorgcentrale, die is ook dag en nacht bereikbaar'.
Antwoord van C op constatering dat die mensen lastiger te bereiken zijn omdat ze niet op één plek zitten: 'Nee, nee. Nou die wijkverpleegkundigen hebben dan wel één keer in de zoveel tijd een teamoverleg met hun leidinggevende, maar ik weet niet precies hoe vaak'.

Samenwerking met communicatieafdeling
C: 'Ja, als ik iets heb dan kan ik met hen contact opnemen. Toevallig, dus daarom kwam dit ook wel mooi uit, was er vanuit het MT de behoefte van goh schrijf nou eens op een A4tje wat belangrijkste speerpunten. Nou daar ben ik mee begonnen, maar met een A4tje kom je niet weg dus dat waren inmiddels drie A4tjes geworden, maar wel punten die ik wel van belang acht en ook gewoon dingen waar mensen thuis mee in aanraking komen hè. Dus toen zeiden ze van he goh misschien moet je eens met communicatie gaan praten en dat is een vrouw die is van extern aangetrokken, we hebben wel een interne communicatie maar die doen meer marketing'.
C: 'Ja iemand voor de PR ook meer aangetrokken. En zij zei ja je zou het kunnen doen met een puzzel van 1000 stukjes beneden neerleggen en dan ontbreken er twee stukjes of nou ja wat meer met een ludieke actie, met wuppies of nou ja ik noem maar wat dat je een wuppie informatiebeveiliging hebt, maar ik ken onze organisatie een beetje en ik weet dat dat in onze organisatie niet echt gaat werken. Ik denk dat als ik daarmee bij het MT aan kom. Ja, dat ze me heel hard uitlachen dus ik zei ik weet niet of ik dat wat vind'.
C: 'En het idee is nu dat is ook van die externe communicatiedame waarvan ik dacht ja dat vind ik wel een goede om een digitaal poppetje te creëren en die af en toe over je scherm te laten komen met een kreet. Weet je dat is niet dat bij iedereen meteen de alarmbellen gaan rinkelen, maar wel dat het iets is wat mensen bij blijft en wel dat dat poppetje dan gekoppeld is aan informatiebeveiliging, dus dat dat gewoon één gezicht gaat worden. Daar kon ik me wel in vinden, ik dacht dat vind ik wel een leuk iets tastbaars waar je wat mee zou kunnen'.

C: 'Ja, maar je zit dan altijd weer met die groep die dan geen scherm heeft'.
Antwoord van C op vraag van onderzoeker of ze vaste computers gebruiken en of je het daarop kunt instellen: 'Ja, ik weet niet hoe dat ICT-technisch zou moeten, maar goed dat zou kunnen. Op laptops zou dat ook moeten kunnen, want wij werken via dat platform en dat kan overal inloggen op je tablet of op je laptop of op je telefoon dus daar zou dat dan denk ik overal op alle devices wel moeten kunnen'.
Alleen dat is bij ons toch wel weer wat anders belegd. Communicatie is hier wat meer ondersteunend aan en de rest moet je eigenlijk zelf maar doen. Het is niet echt zo dat zij, ja weet je je kan ze oproepen als je ze nodig hebt ergens mee, maar zij nemen niet het voortouw van we gaan een campagne opstarten ofzo met dat als onderwerp. En dat is ook weer een beetje omdat dan die prioriteiten weer anders liggen'.
Onderzoeker vraagt waar die prioriteiten dan wel liggen, C antwoordt: 'Ja, dat is voornamelijk ook wel bij uitvoerende, folders up to date houden, foto's'.
Onderzoeker vraagt of het meer extern gericht is dan intern, C antwoordt: 'Ja, nu wel. En ik weet daar zijn ze dan mee bezig, onze afdeling communicatie is bij ons altijd een afdeling geweest die dan daaronder hing en dan daaronder die had nooit echt een vaste plek. Dus veel wisseling ook in leidinggevenden en afdelingen. Ja er zit nu nog maar één persoon en dan een externe, maar ja die heeft andere taken. Dus dat is ja een beetje een ondergeschoven kindje nu'.
Onderzoeker geeft aan dat er dus eigenlijk geen duidelijke plek voor communicatie is en dat dat het ook lastig maakt om met initiatieven te komen misschien C antwoordt: 'Nou nee, daar is geen ruimte voor. Ik vind dat wel jammer hoor, ik denk namelijk best dat ze een grote rol kunnen bijdragen. Ja nu moet je zelf een beetje het wiel uit proberen te vinden en dan ja, is het dan goed, ja ik weet niet of het goed is, maar ja je probeer het beste te doen en je haakt een beetje aan bij andere organisaties en je informeert eens van 'goh hoe zijn jullie bezig' zeg maar.

Bekendheid met 'ZEKER' campagne
C: 'Nee, maar toevallig was dat ook van 'ZEKER'? Las ik vandaag wat, dat ze een mail hadden gestuurd aan 68.000 medewerkers over 28 verschillende ziekenhuizen over die taart, dat ze een taart konden winnen voor een beste zorgteam of de beste zorgmedewerker en dat was dan een fishingmail en dat kon je aan dat mailadres van de afzenders zien en zij brachten dus in kaart hoeveel mensen daarop klikken en op welk niveau wordt er nou toch op die link geklikt. Dus ik heb hem toevallig heb ik hem uitgeprint, en dacht ik die moet ik wel even meenemen want dat vond ik dus wel een hele ludieke manier van bewustwording van ja waar klik ik nou eigenlijk op. nee, maar ik heb niet was dat van zeker?'
Onderzoeker geeft uitleg over 'ZEKER' campagne, C antwoordt: 'Ja die heb ik volgens mij wel, maar dat was volgens mij wel specifiek voor ziekenhuizen of niet? Ja, en volgens mij heb ik hem (de 'ZEKER' test) zelf ook gedaan. Het komt me wel heel bekend voor. Ik denk ook dat die gekoppeld was aan Alert Online he?'
C: 'Nou we hebben nu wel ook aangehaakt op Alert Online, was voor ons ook het eerste jaar dat wij daaraan meededen. Wij hebben toen wel de quiz die zij online ook beschikbaar hebben gesteld die hebben wij ook op ons intranet beschikbaar gesteld voor de medewerkers. We hebben iedere dag bij het inloggen een leus of een tekst kort over informatieveiligheid en dan iedere keer een ander onderwerp met een plaatje erbij'.
Onderzoeker vraagt of dat dan op je scherm komt waar je moet inloggen C antwoordt: 'Ja, dat hebben we aan die campagneweek opgehangen'.

Maatregelen bij niet naleven regels
C: 'Uhm, nog niet, omdat we daar dus nog geen duidelijk beleid over hebben. Toevallig heb ik donderdag daar een afspraak over, daar willen we wel sancties aan gaan ophangen, maar wat voor sancties dat is nog een beetje onduidelijk. Maar daar zijn we wel mee bezig'.

Evaluatie van beleid
C: 'Nee'.
C: 'Ja, als iets vaker voorkomt dan nemen we ze mee. Ja, want we doen ook, issues waarvan ik denk dat we daar wat mee moeten in de organisatie, die koppel ik terug in de stuurgroep en daar geef ik een advies over en dan gaat de stuurgroep de bestuurder die bepaalt dan of hij het advies wel of niet overneemt, dus dat komt wel iedere keer terug in de cyclus'.

Thema in beeld bij bestuur

C: 'Ja we hadden bijvoorbeeld nu afgelopen weekend een datalekincident bij een bewerker. Dat neem ik ook wel gelijk op. Dan koppel ik dat terug naar de bestuurder met mijn advies daarbij van we gaan het wel of niet melden bij de autoriteit, dus die zijn heel dicht betrokken'.
Antwoord van C op de vraag of Raad van Bestuur bepaald of er gemeld wordt of C: 'Ja, ik bepaal, ik adviseer, maar wel met dwang zeg maar om het te melden'.
C: 'Ja, zij zijn eindverantwoordelijk dus ik wil wel graag dat horen en dat op schrift hebben dat hij akkoord is met de melding, maar uiteindelijk adviseer ik wel dringend om dat te melden of om het niet te melden'.
Antwoord van C op vraag hoe Raad van Bestuur dit thema in beeld heeft: 'Ja, alleen middels de stuurgroep'.
Antwoord van C op vraag of de Raad van Bestuur volledig bij die stuurgroep zit: 'Bij ja, we hebben nu voorlopig even een tweehoofdig Raad van Bestuur en de voorzitter zit bij de stuurgroep'.

Risico's in beeld bij bestuur
C: 'Ja, want daar zijn ze ook bij betrokken geweest vorig jaar was er een werkgroep die heeft de risico-inventarisatie gedaan, daar was ik toen nog niet bij betrokken. Ik heb het wel overgenomen en heb de risico's uitgezet bij de probleemeigenaren, overleg mee gehad, gevraagd hè ik heb een opdracht geschreven. Zij moesten aan de hand van die opdracht een plan van aanpak schrijven en ook die wordt iedere keer teruggekoppeld in de stuurgroep en vanuit de stuurgroep gaan ze dan weer mee in het MT'.

Inrichting informatiebeveiligingsbeleid
Antwoord van C op vraag van onderzoeker of het beleid bijvoorbeeld bestaat uit een privacyreglement: 'Ja, dat is onderdeel ervan. Nou we hebben die risico-inventarisatie uitgevoerd waar een aantal risico's naar voren kwamen die zijn onder andere daar benoemd, want ja hoe willen we met die risico's omgaan daar moeten wij als instelling wat van gaan vinden. We merkten dat er eigenlijk ook wel behoefte was aan een algemene gedragscode. We hebben heel veel losse dingen ICT, huisregels, gedragsregels eigenlijk miste daar wat: een algeheel beeld, dus daar zijn we mee aan de gang en ja bewustwording bij de medewerkers dat is bij ons wel een heel groot punt waar we mee bezig gaan. We hebben bij onze ICT-omgeving, zijn we vorig jaar overgegaan naar een platform, dat is helemaal beveiligd, dus die beveiliging zit wel goed, maar ja hoe ga je nou om bij de medewerkers of hoe gaan de medewerkers om met gebruik van Whatsapp en Social Media. Nou daar hebben we niks over'.
C: 'Ja, we hebben een inventarisatie gemaakt papier, techniek en gedrag ik kan het heel even uit de printer halen. Techniek, applicaties, papier en gedrag. Techniek applicaties ging dan voornamelijk over onze grootste applicatie Ons, daar staan medewerkersgegevens, maar ook de cliëntengegevens en ECD zorgplannen en dergelijke, maar daar wordt dan inderdaad gekeken van hoe kan een bewerker bij de gegevens? Zijn ze afgeschermd voor andere gebruikers? Hoe zit het met de uitval van een systeem als een netwerk uitvalt? Maar ook na wateroverlast bijvoorbeeld. Nou daar waren allemaal geen procedures voor. Dus de opdracht was van ga aan de hand van deze risico's maar ook de relaties, afhankelijkheidsrelaties, beschikbaarheidsrelatie, vertrouwelijkheidsrisico, maak daar een plan van aanpak van'.
C: 'Nou en dat is dan gedaan en sommige dingen die behoeven goedkeuring van een bestuurder omdat dat dan begrotingstechnisch ook consequenties heeft. Nou ja sommige dingen kunnen niet uitgevoerd worden en dan wordt beschreven waarom we nu die keuze maken om dat nu achterwege te laten'.
Onderzoeker geeft aan dat ze zich kan voorstellen dat er ook crisiscommunicatie bij komt kijken bij wateroverlast C antwoordt: 'Ja, en dan blijkt ook dat wij dat niet hebben'.
C: 'Dat wij ook geen algemeen calamiteitenplan hebben. Dus naarmate je hiermee verder gaat kom je er ook achter van 'oh dat missen we ook''.
C: 'Ja, dat moet ook dus het is wel leuk dat dat daar uit komt want we hebben dan wel een calamiteitendienst voor het weekend, maar ja als er een echte calamiteit is wat moet er dan gebeuren en hoe gaan we evacueren of wat dan ook, dat hebben we dus allemaal niet'.
Antwoord van C op de vraag van onderzoeker of medewerkers op dit moment wel die gedragscode hebben: 'Ooit een keer gekregen, een keer een 'gebruik ICT' e-mail en daar zet je dan ook een keer een handtekening voor. Nou negen van de tien mensen leest het waarschijnlijk niet. Dus dat willen we ook anders. We willen die algemene gedragscode straks ook door de bestaande medewerkers allemaal opnieuw laten tekenen'.

Procedure Meldplicht Datalekken
Onderzoeker vraagt naar de weekenden C antwoordt: 'Ja, ja. Ik kijk, ik hou dat in de gaten'.

C: 'Nou weet ik wel dat ik was toevallig bij een Ronde Tafel gesprek van de Autoriteit. Ja en toen gaven ze wel aan dat ze die 72 uur niet zo heel dat daar ook best iets langer bij mocht zitten. Ja weet je dat is lastig want ik kreeg bijvoorbeeld afgelopen weekend dat incident. Ik keek heel toevallig vrijdagavond laat op mijn mail en toen zag ik dat er vrijdagmiddag om iets voor vijven een melding binnen was gekomen van onze bewerker. Maar dat betrof wel een incident van de donderdag, maar goed ik heb de melding pas binnengekregen op de vrijdag dus ik heb me daar maar even aan vast gehouden en ik heb toen wel zaterdag contact opgenomen met de stuurgroep en geadviseerd om maandag toch een melding te doen. Dus ik heb uiteindelijk maandagochtend die melding gedaan, dus ik neem aan dat dat prima is gegaan. Het was ook niet een heel ernstig delict ofzo maar ik vond het wel goed om te melden. En dus ja die 72 uur zal zo'n beetje in het weekend, ik check het dan maar wel even of er wat is'.
C: 'Ja, er is een interne meldingsprocedure voor. Ja, staat ook op intranet, daar hebben we een intern meldingsformulier. Dat wordt nog niet zo vaak gebruikt. Het merendeel gaat toch via de mail gegevensbescherming. Daar komt het dan op binnen of op mijn persoonlijke mail. Maar er is wel een intern formulier voor'.
Antwoord van C op vraag of er ook een extern meldpunt is: 'Ja, nee dat hebben we niet voor extern, ja dat staat op onze website misschien, maar dan moet ik even het antwoord schuldig blijven. Het zou kunnen dat we in ons privacyreglement dat het wel benoemd staat en het mailadres gegevensbescherming. En we hebben wel bij de invoering van het ECD, daar waren natuurlijk ook wel veel vragen over van cliënten met name van oudere cliënten hoe zit dat dan en mijn gegevens staan in de cloud en hoe moet ik dat dan zien? Daar hebben we wel een informatiefolder van gemaakt hoe wij daarmee omgaan en daar staat het mailadres ook wel genoemd'.
C: 'En ze weten ook wel dat ze hun eerste verantwoordelijke kunnen aanspreken'.
Antwoord van C op vraag van onderzoeker of medewerkers ook meegenomen worden in het proces als zij een melding doen: 'Ja, ja. Er volgt altijd een terugkoppeling. Hoe we ermee om zijn gegaan.'
C: 'Ja, als er extra vragen zijn bel ik dan ook vaak'.
Antwoord van C op vraag van onderzoeker of nieuwe medewerkers de procedure Meldplicht Datalekken krijgen: 'Ja, dat is nu wel de bedoeling. Dat willen we nu wel opnemen bij indiensttreding of bij de algemene gedragscode dat iedereen dat gewoon krijgt'.

Meldingen
Antwoord van C op constatering van onderzoeker dat het formulier op de website vrij uitgebreid is: 'Ja dat klopt, maar er is wel veel, we hadden van de week dan die melding, dan krijg ik van de bewerker al helemaal een ingevuld formulier, die ik eigenlijk één op één kan overnemen'.
C: 'Wij hebben zelf ook nog geen datalek gehad dat we moesten melden. Maar goed van een bewerker hebben we al wel moeten melden inderdaad'.

Beveiligingsmaatregelen
Antwoord van C op vraag van onderzoeker of er veiligheidsmaatregelen zijn voor mensen die in het weekend werken bijvoorbeeld als je een USB-stick kwijtraakt: 'Beleid is bij ons om niet te werken met USB-stick. Eigenlijk is dat gewoon not done. Iedereen heeft eigenlijk toegang, kan via thuis inloggen. Dat gaat op dat platform dat beveiligd is, dus een USB-stick is not done'.
Onderzoeker vraagt of je overal toegang kunt krijgen tot het systeem en of dat systeem beveilligd is C antwoordt: 'Maar ja dan is het verhaal komt vast ook wel eens ter sprake: je bent aan het werk in het systeem met cliëntgegevens en jouw buurvrouw zit bijvoorbeeld naast jou en die kan bij jou op het scherm kijken'.
C: 'Ja, dat zijn van die dingen. Maar nee USB-sticks mag niet. Is opgenomen ook bij ons in de ondernemingsovereenkomst. Geen gebruik maken van USB-sticks'.

Communicatie-inzet naar aanleiding van Meldplicht Datalekken
Antwoord van C op vraag hoe er bijvoorbeeld gecommuniceerd is over de Wet Meldplicht Datalekken: 'Nieuwsbrief'
C: 'Nee, behalve de nieuwsbrief over de meldplicht datalekken en een stuk op intranet, waar dan het plan van aanpak beschreven staat. En ja ik heb op intranet een stukje geschreven dat die wet is ingegaan en nou ja een informatiebijeenkomst. Dat was dan eind januari, we hebben ook net de medewerkersbijeenkomst achter de rug dat doen we 2x 2 jaarlijks en dan heb je vijf gebieden waar we zitten organiseren we medewerkersbijeenkomsten en dan is dit onderwerp uhm werd ook aangestipt'.

C: 'Ja, één keer per half jaar. Meestal is dat net na de zomer en dan begin van het nieuwe jaar'.
C: 'Ja, iedereen wordt uitgenodigd. Hele wisselende opkomst, je moet niet denken dat er honderden mensen zijn, maar goed. Die bijeenkomst zijn we gestart omdat de werkoverleggen eigenlijk wat geskipt werden vanwege reistijd en productiviteit. En nou ja daar worden actuele zaken besproken, maar dat gaat ook over de financieringssituatie van de organisatie, een beetje dat soort onderwerpen'.
C: 'Ja, we hebben nu dan in november die workshop staan en dat hebben we ook uitgezet hoor van we willen niet droge stof aandragen we willen eigenlijk gewoon aan de hand van stellingen en aan de hand van praktijkcasussen een interactieve sessie hebben. Dus we hebben de vraag ook uitgezet van waar loop jij in de praktijk nu tegen aan. Nou en daar zie je wel dat daar wel reacties op binnen komen, want dat alleen maar stof aandragen en wetten en toestanden ja weet je daar zit niemand op te wachten'.
C: 'Dat is wel weer wat aan de top. Dus het MT, de leidinggevenden, de afdeling finance en control, de ICT-afdeling vanuit daaruit, maar dat kan je aan de hand van stellingen natuurlijk wel leuk doen, kunnen zij het weer meenemen in hun werkoverleg en dan wellicht dezelfde stellingen gebruiken of diezelfde praktijkcasussen'.

Veranderingen in organisatie sinds Meldplicht Datalekken
C: **'**Ja, nu in de loop van het jaar wel, komen er meer vragen. Maar ja weet je dat heeft wel tijd nodig en ik denk ook dat de een daar meer mee bezig is dan de ander. Maar we merken nu wel dat er meer vragen via de mail binnenkomen van goh hoe moeten we nu hiermee omgaan.
Weet je wat het lastige is, wij hebben eind januari een informatiebijeenkomst gehouden, dat was voor het MT-team leidinggevenden hier en de ICT-afdeling, P&O, beleid. Daar waren iets van 30 mensen, die hebben we toen geïnformeerd en je merkt gaandeweg het jaar dat er wel steeds meer bij mij gemeld wordt dat er wel steeds meer vragen vanuit de organisatie komen van goh we hebben sus maar waarom is het zo en kunnen we dat niet anders inregelen en we krijgen mail van een ziekenhuis binnen, weliswaar via zorgmail een beveiligde omgeving, maar wel van een röntgenafdeling, de bespreking van foto's. Nou die zijn gewoon helemaal verkeerd gestuurd, weet je hoe gaan we hier mee om. Dus dat merk ik wel dat was in het begin was er echt radiostilte. Je merkt wel dat er gaandeweg meer over gecommuniceerd wordt dat er wel steeds meer mailtjes bij mij komen. Ja, dat hebben we gaandeweg het jaar wel steeds meer bemerkt'.

Voorbeeld van audit door GGD
Laatst was er bijvoorbeeld iemand van de GGD geweest, een soort van audit/inspectie. Vooraf was toestemming gevraagd, die wilde wat inzage in cliëntendossiers en die cliënten was toestemming gevraagd. Maar op het moment dat ze er waren wilden ze ook inzage in P-dossiers van medewerkers van een betreffende afdeling om te verifiëren of diploma's in orde waren en of de VOG (Verklaring Omtrent Gedrag) aanwezig was. Daar hangt wel een raamovereenkomst boven waar ook wel in beschreven staat dat dat moet kloppen. Medewerkers zouden daarvan in bezit moeten zijn. Degene die erbij zat was er redelijk door overvallen, ja daar hebben wij ook niet echt beleid over geschreven. Wat moeten wij nu medewerkers van tevoren informeren of er inzage in een dossier is ja of de nee en je kan het niet altijd informeren want soms is het steekproefsgewijs. Nu is het achteraf gedaan. Medewerkers waren daar wel een beetje verbolgen, niet iedereen, maar een aantal waren daar wel een beetje over verbolgen. Ja daar moeten we wel iets mee'.

Risico's voor instelling van een datalek
C: 'Nou, weet je ik ben niet zozeer bang voor een datalek, dat kan ons allemaal overkomen. Ik ben er wel van overtuigd dat als je de dingen maar transparant en helder hebt en er gewoon duidelijk in bent en ook in de communicatie naar buiten. Tuurlijk is het heel erg vervelend als het gebeurt en het is heel vervelend als een medewerker een laptop in zijn auto laat staan en zijn auto wordt opengebroken of weet je wat dan ook, maar uhm zolang wij kunnen aantonen dat wij onze omgeving goed beveiligd hebben en ook maar gewoon duidelijk zijn in het melden ook naar de betrokkene eventueel als dat noodzakelijk is, denk ik dat je op zich niet zo'n groot risico loopt. Wel als je het gaat achterhouden en gaat verzwijgen en denkt van we branden onze vingers er niet aan, we houden onze mond maar dicht'.
C: 'Ja, daar kan je denk ik hele grote schade aan lijden als het bijvoorbeeld groot in de krant komt wat de laatste tijd best veel bij gemeentes voorkomt'.
C: 'En zorginstellingen ook. Ja weet je dat wil je niet. Ja weet je je kan heel veel dingen noemen. Maar ik denk ook transparant naar elkaar, maar ook naar ketenpartners. Ja weet je als wij dat voorbeeld dat ik net noemde, als wij van een ziekenhuis gegevens doorkrijgen die gewoon niet voor ons bestemd zijn en waar gevoelige

informatie in staat. Weet je, je kan het heel hoog op gaan spelen, maar je kan ook mekaar gewoon helpen en zeggen hee jongens, wees even alert hè. Of als er een overeenkomst opgestuurd wordt en er zit achter een andere overeenkomst voor een hele andere cliënt van een hele andere zorginstelling. Ik denk dat je eerst moet zoeken naar gewoon ook een samenwerking'.
C: 'Niemand zit te wachten op een boete van acht ton'.
C: 'Ja, kijk het moet niet 100 keer per week voorkomen natuurlijk, want dan heb je zelf ook wel een keer een probleem, dan wordt het ook jouw probleem dat moet je denk ik niet willen. Ik denk dat dat het grootste risico voor onze organisatie is, hoe medewerkers ermee omgaan'.
C: 'Weet je er wordt nog heel veel via WhatsApp verstuurd want dat is makkelijk en dat is ook een risico waar wij ook naar moeten kijken dat niet al onze medewerkers dus een eigen account hebben, want hoe moeten medewerkers dan communiceren? Dan gaat het via de Gmail, ja dat is dus. Daar moet je dus keuzes in gaan maken'.
Onderzoeker geeft aan dat het natuurlijk ook weer geld kost waarop C antwoordt: 'Ja, wat er dan niet is, want dat blijft een lastig probleem'.
Onderzoeker geeft aan dat ze wel iets heeft gelezen over een applicatie waarbij ze Gmail en dergelijke blokkeren C antwoordt: 'Nee, maar dan doen ze het wel via een omweg thuis via Gmail en dergelijke'.

Bijdrage van communicatie aan het inperken van de risico's
C: 'Uhm, ja ik denk dat zij daar wel een rol in kunnen hebben'.

Regionale samenwerkingen
C: 'Nee, niet dat ik weet. Ik heb laatst wel een gesprek gehad met de gemeente en die had ook zoiets van ja eigenlijk moeten we toch een soort ketenoverleg ofzo initiëren. Dus ik zei van nou volgens mij is dat heel goed om het initiatief bij de gemeente te leggen, want die is natuurlijk ook verantwoordelijke voor heel veel zorginstellingen of ja ketenpartners, maar goed diegene zat ook met het ene been in de ene functie en met het andere been in de andere functie maar die wilde dat wel meenemen want die miste dat ook. Nou ja ik ben dan wel een keer bij een ronde tafel geweest dat was georganiseerd door heliview en daar zaten wel, ja dat was meer richting Enschede was dat toen, maar dat was wel interessant gewoon even met elkaar praten van hoe ga je ermee om en ik merk dat dat communicatie intern gewoon echt een heel moeilijk ding is hoor'.

Motivatie van medewerkers om wel te gaan melden
C: 'Ja, dat is bij ons ook lastig, want dat is bij ons net zoals een MIC-melding of een MIM-melding. Dat wordt bij ons nauwelijks gedaan'.
C: **'**Ja MIC is Melding Incident Cliëntenzorg en MIM is Melding Incidenten Medewerker. Dat wordt bijna niet gedaan, omdat men aangeeft ja we vergeten het of we denken er niet aan of ja het is te lastig om het formulier te vinden. Ja weet je verzint 10 excuses geen idee'.
Antwoord van C op vraag van onderzoeker hoe ze erachter komen dat mensen het niet invullen: 'Nou ja want op een gegeven moment ga je kwaliteitsuitvraag doen en dan denk je op zoveel medewerkers en met zoveel cliënten en dan maar zo weinig meldingen dat kan nooit goed zijn.
C: 'En dan ga je dat terugkoppelen en ja weet je we hebben hier ook bijvoorbeeld de MIC-commissie en daar is inderdaad naar gekeken van hoe kan dit anders en dan is er weer ander beleid en het verandert niet. En kwaliteit is hier, het is altijd goed hoor, we hebben altijd een hoog cijfer voor kwaliteit en ook bij de CQ index en noem maar op. Maar het is altijd wel een dingetje en dit is ook een dingetje. We willen dit koppelen aan kwaliteit, omdat wij vinden dat kwaliteit iets moet zijn wat jij in je hebt als zorgverlener. Maar medewerkers ervaren het, vooral de uitvoerende echt als een dingetje'.

Rol van de Autoriteit Persoonsgegevens
C: 'Uh, ja hoe kijk ik tegen die rol aan. Ik vind ze nog niet heel sterk. Ik vond ook dat tijdens die bijeenkomst ze zelf ook niet heel sterk naar voren kwamen, omdat er nog teveel ook onduidelijkheid was, wat je dan merkt is dat je de ene dag belt en je krijgt Jan aan de telefoon en de volgende dag krijg je Pietje, dat ze dan beiden een ander antwoord geven. Ikzelf vind dat hun bereikbaarheid heel slecht is. Ik heb ze een paar keer gebeld en dan kreeg ik een bandje dat er een probleem was of ik weet niet hoe lang ik in de wacht heb gestaan, ze zijn niet per mail bereikbaar. Dat vind ik ook heel vervelend, alleen maar de ochtenduren. Ja, ik kijk er niet tegenop ofzo. Ik vind autoriteit een fantastische naam, maar ik heb niet zoiets van poehpoeh ik lig er wakker van'.
Onderzoeker checkt of ze dus niet makkelijk benaderbaar zijn C antwoordt: C: 'Nee, absoluut niet'.

C: 'Er zijn ook heel veel goede dingen hoor, zoals ik vind hun website goed want als je zoekt op bepaalde onderwerpen krijg je best snel je informatie, kan je boven water halen. En ik moet zeggen dat ik vind dat zij zelf wel wat autoriteit uitstralen in die zin van je durft bijna geen vraag te stellen telefonisch omdat je denkt van oeps weet je wel als ik nu die vraag stel waar ik zelf dan niet uitkom dan krijg je meteen een vinkje bij je naam en dan gaan ze daar naar kijken. Dus ik vind transparantie, dat zou denk ik beter kunnen of anders kunnen'.
Onderzoeker geeft aan dat eigenlijk niemand zei waar die vandaan kwam bij die bijeenkomst C antwoordt: 'Ja, iedereen is dan toch een beetje en dat snap ik he want ik heb ook begrepen dat zij dit ook niet zo heel snel doen. Dat ze dit ook nog nooit eerder hadden gedaan zo'n bijeenkomst waar zij bij aanwezig waren. Terwijl ik juist denk, ja je moet het zo zien. We moeten niet denken met z'n allen dat is de grote politieagent daarboven waar we allemaal bang voor moeten zijn. Ik bedoel zij moeten de wetten handhaven, de regels, wij moeten ons daar als organisatie aan proberen te houden, maar laten we vooral heel open en duidelijk tegen elkaar zijn want ja, niemand zit te wachten op, zij zitten ook niet te wachten op een boete uitdelen, want als zij een boete uitdelen daar krijgen zij ook gedoe mee of gedoe mee, dan gaat iedereen ook zeggen ja nou ze hebben hun natje gehaald'.
Onderzoeker geeft aan dat het wel een bewuste keuze is van de AP om als toezichthouder op te treden en niet als advies/raadgevend orgaan en dat er over te twisten valt of dat een goede keuze is en dat de boetes nog niet aan de orde zijn geweest C antwoordt: 'Nee, ongetwijfeld zal er snel eentje gaan komen'.
Onderzoeker geeft aan dat het misschien ook niet heel handig is om meteen boetes uit te delen, omdat minder mensen dan gaan melden C antwoordt: 'Ja dat is de andere kant van het verhaal, die boetes zijn zo enorm hoog. Ja weet je als je als organisatie een boete krijgt dan is het einde. Tenminste bij zorginstellingen gaat het nu niet zo heel fantastisch allemaal'.

Voorbereiding op de AVG
C: 'Nou wij hadden een mooi schema, had ik gevonden en daar stond dan in wat zijn nu de grootste veranderingen, maar naar aanleiding van de Ronde Tafel bijeenkomst heb ik hier het advies gegeven om vooral nu nog even niets te doen, want de autoriteit gaf zelf aan dat het voor hen ook nog niet helemaal duidelijk is wat nu de kaders zijn en wat voor richtlijnen zij daaraan gaan hangen en dat zij ook met iets naar buiten willen gaan komen. Dus ik heb hier als advies gegeven ja weet je we kunnen het beste jongetje van de klas willen zijn en ons helemaal daar nu op gaan richten, maar zolang de autoriteit daar nog niet echt verder mee naar buiten is getreden, laten we het even zo houden. Want door allerlei commerciële partijen wordt je benaderd wordt je doodgegooid bijna met trainingen en cursussen en opleidingen, maar dan denk ik laten we eerst eens duidelijk hebben wat zo'n autoriteit daar nou mee wil beogen'.
C: 'Vond ik bijzonder om te horen tijdens die bijeenkomst. Ja, weet je zolang zij daar nou nog niks over hebben'.
C: 'Ja, maar volgens mij speelt er nog wel is er nog wel wat variatie in in te brengen. Natuurlijk zijn wij, we hebben natuurlijk mij aangesteld als FG, alle gegevensverwerking moet gedocumenteerd worden wat natuurlijk eerst niet zo was. Daar zullen we een slag in moeten maken want dat is nu nog niet. Als ik daar kijk naar het formulier dat de autoriteit handhaaft dan denk ik van nou dat is zo'n stapel papier, waar ze dan wel een programmatje voor hebben, maar ik weet zeker als ik dat hier ga uitzetten dat de helft van de mensen niet weet wat ze moeten invullen dus daar moeten we eerst eens kijken of we daar een schift in kunnen maken en dan misschien geven zij daar zelf ook wel een ander handvat aan. Dus ja, weet je, we hebben zoiets nu van, we wachten heel even af wat de autoriteit hiermee gaat doen'.

6.4 Categorisatie Interview zorginstelling D

Achtergrond van de Functionaris voor de Gegevensbescherming
D: 'Ja, eigenlijk omdat ik als jurist hier werk en eigenlijk als je kijkt naar het functieprofiel van FG dan zit daar best heel veel overlap in en als je dan verder in de zorginstelling kijkt van ja waar kun je het beleggen dan leek dit de meest aangewezen plek'.
D: 'Het onderwerp privacy en beroepsgeheim en dat soort zaken, ja dat lag toch al bij mij, dus het is in die zin een heel erg pragmatische keuze geweest om het aan de functie van de jurist te koppelen'.

Belegging van de functie in de organisatie
D: 'Ja, dat is een spannende vraag, want we hebben net een reorganisatie gehad en uhm ja het meest duidelijk is; ik val vrij direct onder de Raad van Bestuur. Er zit nog een directiesecretaris zit daar dan nog functioneel tussen zeg maar voor de arbeidsvoorwaardelijke zaken enzo, maar ik zit niet meer bij een organisatieonderdeel, maar het zit heel dicht tegen de Raad van Bestuur'.

Antwoord van D op opmerking van de onderzoeker dat het natuurlijk ook een onafhankelijke functie is: 'Ja en dat is ook de reden waarom ook nu na de hele reorganisatie ervoor gekozen is om de functie jurist ook daar te laten, omdat je dan toch het meest onafhankelijk kunt functioneren in de organisatie'.

Inrichting informatiebeveiligingsbeleid
D: 'Ja, kijk privacy is natuurlijk in de GGZ altijd al een belangrijk thema geweest, dus het is niet zo dat er nu in één keer nu de nieuwe wetgeving er is, dat iedereen zo zit van 'oh we moeten van alles', uhm, ja ik ben zelf als het om nieuwe wetgeving gaat dan vaak wel degene die daarop wijst of initiatief neemt of stukken daarover schrijft, uhm ja verder kan het van allerlei kanten komen waar privacy speelt. Ik denk wel dat nu met de Wet Datalekken, maar ook de hele ontwikkelingen rond bestuurlijke verantwoordelijkheid, dat dit thema wel een soort professionaliseringsslag meemaakt. Zeg maar dingen die ik vind dat ze vrij hapsnap een beetje adhoc geregeld zijn in een organisatie daar gaat nu meer gekeken worden naar het integrale beleid zeg maar. Dus we hebben wel allerlei documenten over privacy, beroepsgeheim, over wat je wel en niet mag en moet, maar ja het is natuurlijk zo breed, het zit natuurlijk overal in dus je wilt ook het totaalplaatje'.
D: 'Nou ja het is goed om even uit te leggen die FG functie is ongeveer een jaar geleden ingesteld, ja toen heb ik ook aangegeven dat is ook belangrijk dat we weten waar we nu staan hè want ja ik kan wel zogenaamd toezicht gaan houden, maar als we niet eens weten wat de nulmeting is, want ik wist natuurlijk vanuit mijn functie als jurist wel heel veel aspecten, maar het totaalplaatje was er niet. Dus we hebben een extern bureau een privacy impact assessment laten doen. Nou daar hebben ze een eerste stap in gedaan, een soort grof overzicht en één van de zaken die daaruit kwam was inderdaad dat er een soort awarenesscampagne moest komen. Dus daar zijn we nu met de afdeling communicatie net in gestart om dat op poten te zetten, dus dat heeft nog niet een echte inhoud, maar toevallig zit dat externe bureau dat daar onderzoek gedaan heeft, zit vandaag ook hier weer voor stap twee en dan even nog meer specifiek kijken naar voldoen we aan de wettelijke eisen en normen vanuit de NEN enzo en de Wet Datalekken en nou ja noem maar op. Dus dan is er ook een soort totaalplaatje straks van waar schieten we nog tekort en ik denk dat we in technische zin zaken wel redelijk goed voor elkaar hebben hè. Je kunt hier echt niet zomaar een patiëntendossier in hoor daar moet je echt wel voor geautoriseerd zijn en zoveel wachtwoorden ingevuld hebben, maar de awareness, dus het informeren van mensen van wat mag je nou wel en wat mag je nou niet, het toezicht en het sanctiebeleid, die punten daar vind ik zelf van daar moeten we nog wel mee aan de slag'.

Communicatie-inzet informatiebeveiligingsbeleid
Antwoord van D op vraag van onderzoeker of de voorlichtingscampagne specifiek gericht is op datalekken of meer op het algemene privacy: 'Dat zal beiden zijn, ja we hebben nu één gesprek gehad met communicatie en nou ja het woord campagne wordt al meteen is dat nou wel de juiste term, want campagne is kortdurend begrijp ik in jullie termen in jullie vakgebied'.
D: 'Nee precies, dus het zal een campagne worden met verschillende aspecten, waarin we het principe van datalekken en het melden ervan op een redelijk eenvoudige manier nu naar voren willen brengen door toch heel kort uit te leggen van nou ja wat is het en wat doe je? Bij wie meld je dat? En wat gebeurt er dan mee? Maar het hele privacyaspect dat zal een doorlopende informatie moeten zijn.
Antwoord van D op de vraag of er nu al iets aan medewerkers wordt overgedragen over privacy: 'Nou, niet heel veel anders dan wat ik zei via dat digitale documentatiesysteem en ikzelf word wel eens uitgenodigd op een afdeling om iets erover te vertellen en dat gaat dan meestal vanuit de regels vanuit het beroepsgeheim zeg maar, wat mogen we nou wel delen en wat niet'.
Antwoord van D op de vraag op welke manier de voorlichting wordt ingestoken: 'Nou we hebben een intranet dat is altijd een belangrijk medium voor nieuwsberichten. We hebben ook een intern magazine dat met enige regelmaat uitkomt dus daar kun je dingen inzetten. En ja verder kan ik wel gaan fantaseren maar hebben we het niet uitgewerkt, dus wat dat betreft ben je net iets te vroeg omdat we nu nog eigenlijk ik en het hoofd informatiemanagement zijn nu communicatie aan het voeden met informatie en zij komen dan met een plan'.
D: 'Nee, zeg maar het meer push met posters of nou ja via nieuwsberichten etcetera dat moet nog. Maar dan verschijnt altijd de voorste pagina van het intranet en daar staan ook de nieuwsberichten op en van daaruit kun je doorklikken naar de patiëntendossiers of naar de documenten'.
D: 'Uhm, wat hadden we afgesproken? Ja er was één aspect dat wilden we nog dit jaar starten, dat was die datalekken, daarbij hadden we echt zoiets van dat willen we zo snel mogelijk doen'.

Relatie met de gemeente

D: 'Nou ja weet je over communicatie gesproken wat dat betreft gemeentes die willen graag dat wij heel veel delen met andere partijen en zij hebben ook een partij die zij inhuren en die hebben een hele mooie leertuin en die promoten eigenlijk dat je veel meer kunt delen dan wat wij als gezondheidszorgveld vinden. En dat is dus ontzettend moeilijk want de mensen op de werkvloer worden er nu mee geconfronteerd met vanuit de ene kant mensen vanuit de gemeente die zeggen van 'goh jullie mogen veel meer delen hoor het is ons verteld door een jurist en het mag allemaal', terwijl ja, ze ook van mij horen, maar ook van de brancheverenigingen en de beroepsvereniging van nee dat is niet zo je hebt je gewoon te houden aan de regels van het beroepsgeheim en dan zie je mensen dus verschrikkelijk worstelen want ja je zit wel aan tafel met elkaar en de één zegt 'goh vertel mij eens even ken jij die persoon?' En dat is al de basisvraag waarvan degene met beroepsgeheim al moet zeggen 'ja joh dat mag ik je niet zomaar vertellen of ik iemand ken of niet'. Het feit alleen al dat iemand bij onze instelling ingeschreven staat valt al onder het beroepsgeheim'.
D: 'Nou ja, zij zien dat als uitvloeisel van de wettelijke opdracht die zij hebben gekregen om in het sociale domein voorzieningen te treffen en daar zorg te verlenen, maar zorg gaat veel verder dan de geneeskundige zorg en wij zitten met die individuele geneeskundige zorg binnen het medisch beroepsgeheim, maar degenen die meer algemene voorzieningen doen, die hebben natuurlijk ook wel te maken met privacy, maar die kunnen dat nog iets ruimer opvatten dan binnen medisch beroepsgeheim'.
D:' Nou ja en dat stelt ons natuurlijk helemaal niet gerust als je denkt aan hoe moeilijk het is in zo'n organisatie als dit om dat dicht te timmeren, terwijl er over het algemeen best wel veel bewustzijn bij mensen is denk ik dat je niet wilt dat er een psychiatrische geschiedenis op straat ligt, ja dan maak ik me wel eens zorgen hoe gaat dat bij de gemeentes?'

Verhouding tussen privacy en de bescherming van persoonsgegevens
Antwoord van D op vraag van onderzoeker of er onderscheid gemaakt wordt tussen die twee: 'Nou, ja, ik zou bijna zeggen het liefst zo min mogelijk. Kijk privacy is natuurlijk een enorm containerbegrip, maar aan de andere kant als je dan voor mensen onderscheid gaat maken tussen persoonsgegevens en privacy dan wordt het voor de medewerkers weer heel lastig'.
D: 'Dat merk ik nu al met datalek, daar zitten we nu ook, daar zijn we bezig met een voorlichtingscampagne daarover om mensen er ook van bewust te maken dat ze dingen moeten melden en ja dan moet je gaan uitleggen ja wat is een persoonsgegeven en dan weten mensen het wel maar als je dan een definitie opschrijft, daar worden mensen niet gelukkig van'.

Informatie over de instelling
D: 'We zijn met ongeveer 2400 medewerkers nou weet ik het niet precies maar volgens mij zijn iets van tussen de 1400 en 1600 daarvan hulpverleners, ja dat varieert van psychiater, psycholoog, verpleegkundigen, agogen, verzorgenden en verder ja secretarieel staf'.

Verschillende benaderingswijze voor verschillende groepen
D: 'Ja, kijk, ja hoe moet ik dat zeggen. We hebben een elektronisch documentensysteem en daar staat alle informatie daar staan alle beleidsafspraken en regels in. Nu is dat natuurlijk een vrij statisch iets, daar moeten mensen al de moeite voor nemen om in te gaan kijken en die richten zich, de meeste regels richten zich toch wel op de zorgverlening en er is een handboek administratie en daar staan ook wel dingen in voor administratieve staf enzo'.
D: 'Nee, dat is in de communicatie altijd lastig we hebben een enorm groot gebied, dus het is een hele grote regio met geloof 60 locaties of zoiets. En ja je moet dus mensen, je kunt ze niet allemaal persoonlijk benaderen. Je kunt niet zeggen van goh nou nu gaan we een middag organiseren en dan komt iedereen dat lukt niet. Dat is natuurlijk sowieso al moeilijk in de zorg, maar het zal dus toch vooral via elektronische weg moeten of papier. Ja, daar blijf je ook deels afhankelijk van ja is er de wil van mensen om het tot zich te nemen, want niet iedereen staat op dezelfde manier in z'n werk hè sommige mensen denken ook ik doe m'n werk en ik ga weer naar huis, klaar. Dus ja dan kun je het bijna onder de neus wrijven, maar he ik vind even vanuit de werkgever geredeneerd wij zijn verplicht om mensen zo goed mogelijk voor te lichten en ja als mensen dingen dan vervolgens niet goed doen dan kun je in ieder geval nog zeggen ja we hebben wel ons best gedaan om mensen dat bij te brengen, erop te wijzen dus ja werknemers hebben daar uiteindelijk ook een eigen verantwoordelijkheid in'.

Thema in beeld bij bestuur

D: 'Uh Ja, want we hebben een afdeling informatiemanagement, met dat hoofd zet ik het nu op en we hebben inmiddels maandelijks overleg met één van de directeuren met één van de bestuurders over nou ja wat is nu de stand van zaken en daar zit natuurlijk het mechanisme achter, daarachter zit de Raad van Toezicht die ook willen weten wat is de stand van zaken. En dat is wel dat merk je bij zo'n Wet Datalekken er wordt met hoge boetes gedreigd en dan ontstaat er een soort schrikeffect ook bij bestuurders zo van hebben we het wel op orde'.

Prioriteit van privacy in de organisatie

Een simpel iets, nou er staat duidelijk opgeschreven dat je geen persoonsgegevens naar privé-emailadressen moet sturen, alles moet binnen het netwerk van ons blijven. En ik hoorde nu gisteren toevallig weer dat vanuit hoger management nog daar onbekendheid mee was dat er tegen een medewerker werd gezet, nou dan stuur je het toch even naar je huismailadres. Technisch lukte het intern even niet dan was het van nou dan stuur je het toch even'.

D: 'Nou dan val ik bijna van mijn stoel: hoe kan het dat iemand vanuit hoger management dit zegt? Dit is voor mij zo'n basisregel, waarvan ik best wel eens begrijp dat er misschien ook wel bewust een keer voor gekozen wordt om dat niet te doen, maar nou ja dan denk je nog dan overtreden mensen bewust de regel, maar onbewust regels overtreden, ja dan wordt het wel, dan moeten we toch wel aan de slag om het mensen helder te maken'.

D: 'Ja, wat ik gezien heb toen deze wet eraan zat te komen dat ook vanuit commerciële hoek de angst enorm vergroot is. Er zijn echt advocatenkantoren en andere kantoren geweest die met name op bestuurlijk niveau enorm de angst gevoed hebben. Pas op, als jullie het niet op orde hebben dan… En let u wel even op uw persoonlijke bestuurlijke aansprakelijkheid hierin en ja het was allemaal niet gelogen maar het was ook toch wel veel bangmakerij om toch werk te krijgen vond ik hoor. Zo van als jullie je bewerkersovereenkomsten niet op orde hebben dan… En dat is heel specialistisch werk, terwijl er ondertussen al standaard bewerkingsovereenkomsten circuleerden die ja, voor 90% gewoon goed zijn en dan moet je nog een paar dingetjes voor je persoonlijke aanpassen'.

D: 'Ja, dus ik heb wat dat betreft ook meer moeite gehad de directie hier gerust te stellen zo van ja dat valt allemaal wel mee'.

D: 'Ja, vind ik wel. Nee, het heeft hoge prioriteit. Natuurlijk vinden allerlei slordigheden plaats, dingen waarvan je denkt dat kan beter niet. Maar ja wij hebben zo'n 20.000 patiënten per jaar en als je dan kijkt naar het aantal incidenten die in ieder geval bij mij bekend worden dan is dat niet veel. Dan denk ik van nou met 2400 medewerkers. Het leidt niet heel vaak tot ernstige incidenten waarvan je echt denkt van nou dit is echt heel erg'.

Onderzoeker geeft aan dat het natuurlijk ook zo kan zijn dat mensen het niet melden D antwoordt: 'Nee, daar ben ik me absoluut van bewust dat heel veel niet gemeld wordt de kleine dingen, maar dan is blijkbaar degene die het betrof of het heeft niet geleid tot iets of degene die het betrof heeft ook zelf gezegd van nou ja kan gebeuren, want dat is natuurlijk ook wel heel vaak zo'.

Risico's voor instelling van een datalek

D: 'Ik denk het grootste risico als instelling is natuurlijk de imagoschade die je op kunt lopen en eventueel de financiële schade maar goed dat zou dan zijn als iemand een schadeclaim in gaat dienen, maar het zou natuurlijk plat gezegd heel gênant zijn als patiëntgegevens op straat komen te liggen'.

D: 'Uhm, nee, nou de grootste kwetsbaarheid hè als wij daar met de interne deskundige over nadenken is de menselijke factor. Technisch is het wel dichtgespijkerd, zelfs als je er het beleidsdocument op na slaat dan denk je nou dat ziet er allemaal wel netjes uit, maar mensen moeten zich er ook naar gedragen, dus dat betekent dat mensen moeten weten wat ze wel en niet mogen en dan ook nog doen.

Procedure Meldplicht Datalekken

D: 'Nou ja het staat nu wel in het privacydocument dat je een datalek moet melden bij de functionaris gegevensbescherming, dus dat ben ik. Maar goed we willen nog zowel in de campagne als in een apart schemaatje dat nog wat versimpelen zeg maar'.

D: 'Eigenlijk is het de bedoeling dat ze twee dingen doen: we hebben een incident-meldsysteem en daar kun je ook beveiligingslekken melden, dus het moet in dat systeem gedaan worden. Dat zou ik dan kunnen zien, maar ja de praktijk is dat die mailtjes niet altijd zomaar. En je moet binnen 72 uur eigenlijk reageren hè. Dus het idee is eigenlijk dat als iemand iets kwijt is geraakt dat diegene dat meldt bij zijn leidinggevende en dat de

leidinggevende het meldt bij mij. Ja, we hebben het niet over anoniem melden gehad, ja dat is ook heel erg lastig want je hebt informatie nodig van ja wat is er gebeurd? Heb je het verteld aan degene die het betreft? Kijk en het idee van incidenten melden is natuurlijk dat dat niet leidt tot sancties, tenminste niet het melden zelf'.
D: 'Dus je probeert vooral te onderzoeken van hoe kunnen we voorkomen dat het weer gebeurt?'
D: 'Ja, ja dat zei ik dat systeem waarop je agressiemeldingen of valincidenten doet. Dat zit in één systeem en je kunt gewoon kiezen wat voor soort melding je doet, dus dat systeem kent men wel'.
D: 'Ja en je zit ondertussen er wel een beetje mee dat wanneer het gaat om incidenten melden dat het geregionaliseerd is hè dus er zijn nu mensen op locatie die meldingen afhandelen. In het begin ging dat allemaal heel erg centraal en nu is er de gedachte, ja als er een incident is dan moet je dat vooral op de afdeling waar het gebeurd is in eerste instantie afhandelen. Dus er zijn daar ook nu mensen die daar bewust mee bezig zijn en hopelijk ook collega's daarop wijzen'.

Evaluatie van incidenten
Onderzoeker vraagt of er geen casussen besproken worden D antwoordt: 'Nee, als er een groot onderzoek is geweest omdat er een calamiteit is geweest. Dat komt niet op intranet van goh dit zijn de bevindingen geweest en dit zijn de verbetermaatregelen en hé jongens wil iedereen daar even op letten, terwijl dat in mijn ogen wel goed zou zijn om dat wel te doen. Je moet natuurlijk altijd oppassen dat je ook niet de privacy van de medewerkers schendt en dat soort zaken, maar ja met een beetje goede wil'.
D: 'Maar ik denk dat er toch angst is dat zo'n bericht ook als je dat intern doet dat dat ook naar buiten gaat. Ja, zoals wat gisteren met zo'n verpleeghuis was hè zo'n plascontract'.

Communicatie-inzet naar aanleiding van Meldplicht Datalekken
Onderzoeker vraagt aan D of de medewerkers daar dan niet meer in getraind hoeven te worden D antwoordt: 'Nee, daar zijn in het verleden campagnes op geweest en dat werkt'.
Onderzoeker vraagt door hoe die campagnes in het verleden werden ingestoken en wat toen gedaan werd D antwoordt: 'Oeh, dat is alweer een paar jaar geleden. Uhm, ja eigenlijk wel dezelfde kanalen als die ik zonet noemde. Dat was dus via intranet, maar ook naar managementoverleggen gaan waar mensen met het team dan zitten. Je hebt vaak wel één keer in de veertien dagen ofzo werkoverleg dat je je daar laat uitnodigen en dan uitlegt van joh dit systeem is er en wil je medewerkers daarop wijzen dat ze dit systeem gaan gebruiken'.

Lastige punten om beleid door te voeren
D: 'Nou ja, wat je ziet is hè af en toe gebeurt er een incident of een calamiteit. Dat waar dat gebeurd is, is er altijd een enorme awareness bij zo'n afdeling en dan hoef je niemand meer voor te lichten, die mensen weten het allemaal precies. Alleen hoe draag je dat dan over naar de rest van de organisatie en dat is moeilijk. En ik verwijt ons ook wel dat we niet echt een hele goede lerende organisatie zijn. Ja, dat is niet bewust, maar om nou te gaan zeggen van 'ja goh let erop want daar en daar is dit misgegaan'. Dat is toch een beetje als je vuile was buiten hangen'.

Voorbeeld van het plascontract
D: 'Ja, er kwam in het nieuws dat wanneer mensen in een verpleeghuis kwamen dat mensen dan iets moesten ondertekenen dat ze drie keer per dag mochten plassen'.
D: 'En dat lijkt natuurlijk heel erg ernstig, maar gisteravond toen werd dat door de directeur van dat verpleeghuis ook wel heel erg genuanceerd van nou ja dit is helemaal uit zijn context gehaald en daar zie je dus dat voor je het weet tegenwoordig met moderne media dat als iets niet goed is je er heel weinig greep op houdt om dat nog te corrigeren'.
D: 'Zeg maar een soort zorgplan waarin dan stond van u mag drie keer per dag naar de wc ofzo. Ik heb de discussie ook niet helemaal gevolgd, maar dat lijkt natuurlijk bizar dat als je in een verpleeghuis wordt opgenomen dat je dat moet ondertekenen. Zo werd dat een beetje gebracht van nou je moet eerst dat ondertekenen dan mag je pas in het verpleeghuis komen, nah dat bleek allemaal veel genuanceerder dat ging erom dat je op een gegeven moment wel wat structuur moet aanbrengen in de dag, er zullen soms dementerenden wel 36 keer per dag naar de wc moeten, maar dit was niet zoals het is gebracht. Ondertussen dan reageert de minister al en dat is natuurlijk ook de angst voor een organisatie als dit van als er dingen op straat liggen, ja dat heb je niet meer onder controle. De nuancering raakt heel snel kwijt. We hebben ook wel incidenten gehad waar mensen naar de televisie gingen en bij de EO op de vijfde dag ofzo kwam het en dan

denk je soms ook van ja dat gaat wel heel erg ongenuanceerd en daar ben je dan natuurlijk niet zo blij mee als dat zo is. Anderzijds zijn we er ons als organisatie ook wel heel erg van bewust dat transparantie de norm is tegenwoordig, je moet gewoon heel erg transparant zijn. Tegenwoordig als we calamiteitenplannen opstellen dan zullen we dat altijd delen met betrokkenen en familie en dat ja als de familie ermee naar de pers stapt dan tsja dat is dan maar zo'.
D: 'Nee, maar daar hoop je dan inderdaad op dat er ergens in de wereld iets heel ergs gebeurt. Maar wat ik wel echt een probleem vind is wat jij net zelf ook zei: het kan iets doen met de bereidheid van mensen om eerlijk te vertellen wat er gebeurd is. Mensen wordt gevraagd in zo'n onderzoek, vertel wat er gebeurd is het is niet bedoeld om je daarna een tik op de vingers te geven maar om ervan te leren hè hoe kunnen we dit nou in de toekomst voorkomen. Maar als mensen weten dat het straks op straat ligt, dan heb je het risico dat mensen toch terughoudender worden hè. Je wilt ook niet straks van journalisten een microfoon onder je neus krijgen'.

Maatregelen bij niet naleven regels
D: 'Nou nog niet expliciet en daar moet, dat is ook wat ik zei één van de aspecten het sanctiebeleid laten we maar zeggen, dat moet duidelijker omschreven worden. Er zijn wel incidenten geweest dat mensen onrechtmatig in dossiers keken en dat dat natuurlijk bekend werd toen. Ja in één geval heeft dat geleid tot ontslag en in een ander geval tot een ernstige waarschuwing. En dan zie je dat omstandigheden net wat anders waren, waarbij je bij de één zegt ja daar was eigenlijk al een keer voor gewaarschuwd, maar dan is het gewoon via de algemene regels, arbeidswetregels worden dingen afgehandeld, maar mensen hebben natuurlijk eigenlijk wel recht om dat van tevoren te weten nou als je dat doet dan loop je dit en dit risico'.
Onderzoeker vraagt of er ook gedragscodes zijn in deze instelling: 'Uh, dat is een goede vraag. Ja, maar die gaan niet zover als op dit. Dat gaat veel meer over gedrag en hoe je met elkaar omgaat'.
D: 'Nou kijk, mijn twijfel is natuurlijk meteen als er gedragscodes zouden zijn dan zou ik ze moeten kennen, maar vraag mij niet. Ik weet dat er oneindige discussies zijn geweest over gedragscodes en nou ja iedereen vindt daar wat van. Als je me nu zegt van welke zijn het, geen idee'.
D: 'Maar ik denk dat er in de psychiatrie zeker en misschien in de zorg in z'n algemeen ook wel een bewustwording is dat mensen snappen dat je informatie niet op straat legt'.

Bijdrage van communicatie om risico's in te perken
D: 'Ja, dat is denk ik heel erg belangrijk omdat de regels ook aangescherpt zijn en ja zeg maar toch het naar voren brengen van dit aspect. Kijk het lastige is in zo'n zorgorganisatie zijn zoveel aspecten waarover mensen geïnformeerd moeten worden dat je als organisatie ook keuzes moet maken van waar leggen we nu de nadruk op? De zorg verandert steeds ook de regels veranderen steeds en overal moeten mensen over geïnformeerd worden en alles lijkt belangrijk als je er mee bezig bent en medewerkers worden echt overvoerd met informatie, die worden daar helemaal gek van van 'goh heb je dit weer dan heb je dat weer''.

Samenwerking met communicatieafdeling
Antwoord van D op vaag van onderzoeker wie de keuzes maakt in welke informatie wordt verstrekt aan medewerkers: 'Ja, communicatie in samenspraak met de Raad van Bestuur maar soms ook de waan van de dag, zo'n datalekwet die er dan ineens komt die financiële risico's met zich meebrengt'.

Aandacht in de media
D: 'Ja, veel te veel vind ik ook hoor, want ik merk dat de regelgeving eigenlijk heel onduidelijk is, eigenlijk weten we niet wat we wel en niet moeten melden en dan zie je omdat er in theorie zo'n hele grote boete tegenover staat dat we dus alles melden. Laatst was iemand, was er een ID-kaart gestolen van een patiënt, ja dat heb je dan maar gemeld, want ja als je de regels nagaat dan moet je dat melden hè, het zijn bijzondere gegevens want het zijn patiëntgegevens BSN-gegevens, ja moet je melden, maar ik geloof zelf nooit dat die wet daarvoor bedoeld is, die wet was veel meer bedoeld voor grote inbreuken'.

Beveiligingsmaatregelen
D: 'Ja, daar is in zoverre beleid voor het systeem laat het ook niet toe om usb-sticks te kopiëren maar er is natuurlijk altijd de omweg dat je iets kunt e-mailen naar je eigen adres en dan op een usb-stickje kunt zetten. We hebben toevallig ook vorig jaar een verbeteractie gehad met de ja mensen die hier onderzoek doen, wetenschappelijk onderzoek vanuit de opleiding. We hadden wel SPSS losse versies, maar die stonden dus op laptops die mensen dan meenamen en dat vonden we wel een risico en mensen vonden het zelf dan ook wel

weer lastig, dus die gingen dan vaak gegevens overhevelen naar de universiteitsserver dan konden ze daar op SPSS werken. Nou ja dat hebben we verbeterd door een netwerkversie aan te schaffen, waarin mensen die wetenschappelijk onderzoek doen dus via het netwerk op SPSS terecht kunnen. Dus niet meer extern hoeven te doen, ook niet thuis, want je kunt dus ook thuis inloggen op het systeem'.
D: 'Ja, je kunt overal op de wereld in principe inloggen in het systeem. Dat is beveiligd en dan zit je gewoon binnen het beveiligde systeem van onze instelling en daar heb je natuurlijk meer mogelijkheden en daarbij is ook een protocol geschreven voor het anonimiseren van gegevens van hoe doe je dat en dus wanneer vinden wij dat het geen persoonsgegevens meer zijn'.
D: 'Nee maar wat je hier natuurlijk soms hebt is dat mensen gegevens willen hebben, maar die komen natuurlijk uit een patiëntenbestand en die moeten geanonimiseerd worden en niet iedereen die deed dat op dezelfde manier en af en toe kon je gewoon het ene met het andere nummer weer combineren en dan wist je precies wie het was, ja als ze bijvoorbeeld het patiëntennummer laten staan bijvoorbeeld'.
D: 'Ja, het meeste onderzoek is hier natuurlijk onder patiënten en dat is al één ding want dat moet dan natuurlijk uit databases gehaald worden en dat dan die dingen zo geanonimiseerd worden en soms deden ze dat ook pas als ze die dingen al thuis hadden staan. En daar hebben we afspraken over gemaakt van hoe dat anders moet'.

Veranderingen in organisatie sinds Meldplicht Datalekken
D: 'Nou, op bestuurlijk niveau is er wel heel veel aandacht voor geweest. Ik heb natuurlijk zelf heel veel vragen gekregen als jurist 'joh waar staan we en wat zijn onze risico's?' Dus daarom is ook die functie van FG ontwikkeld, maar in de organisatie zelf is daar nog niet zo heel veel aandacht voor geweest. Ja, ik heb wel eens een keer een nieuwsberichtje over het feit dat er een FG is en wat dat dan betekent geschreven, maar ja dat is één berichtje en een week later is het weg en dan zullen mensen het weer vergeten zijn. Het is wel opvallend dat wanneer je zo'n bericht neerzet dat je dus die week ontzettend veel vragen en meldingen krijgt op iets'.

Voorbeeld van een incident
Zorginstelling D: 'Ja, wat dat betreft, maar dat was nog voor de wet datalekken, hadden we ook wel een mooi, of nou ja een mooi incident, ook voor dat mensen vragenlijsten moeten invullen voordat ze in zorg komen en sommige mensen hebben geen e-mailadres en dan moest het in het softwaresysteem moest iets ingevuld worden en daar hadden ze ook een afspraak over gemaakt wat je in moest vullen, maar ergens op het secretariaat hadden ze bedacht we bedenken zelf wel even een e-mailadres. En dan bleek dus het vervelende te zijn dat dat een bestaand e-mailadres was en dat kwam dus bij een bedrijf terecht en ja die man kreeg dus in één keer allerlei mailtjes en daar stond dus wel de naam en geboortedatum van iemand in dus ja dat was ja daar ging natuurlijk van alles mis, want ja die mailtjes van die man die bleven ergens in de postbus haken wat niemand zag enzo dus die man werd op een bepaald moment boos. Zo van, als jullie nou niet stoppen dan ga ik naar de pers en dat soort dingen en dat is dus wat je echt niet wilt, ja maar goed. Toen hoefden we dat nog niet te melden dus toen hebben we het wel gecorrigeerd en die man onze excuses aangeboden, maar ja hij heeft ook gezegd ik heb dat allemaal vernietigd en weggegooid ja dat moet je dan maar hopen'.

Meldingen
D: 'Ik heb nu drie meldingen gedaan bij de Autoriteit Persoonsgegevens. Toevallig kwamen er twee weken geleden twee in één week, maar ik denk dat dat een enorme onderregistratie is. Omdat je omdat we er toch voor kiezen om ook de kleine incidenten te melden, dus hè als iemand een e-mail naar het verkeerde adres stuurt, ja dan heb je eigenlijk al een datalek hè als daar nog persoonsgegevens in staan'.
D: 'Nee, ik denk dat dat fors toeneemt. Laatst hoorde ik een instelling die hadden een lijstje met patiëntnamen was op de printer blijven liggen en dat was daar een uur of twee uur blijven liggen en toen werd ie weer gevonden en dat was in een publieke ruimte geweest en toen hebben ze het toch gemeld ook al lag die nog gewoon op het kopieerapparaat van ja in theorie kan het zo zijn dat iemand dat papiertje gepakt heeft door de printer gedaan heeft en een kopie meegenomen heeft. Ja, als je dit soort dingen, strikt genomen moet je het melden, maar daar zit volgens mij niemand op te wachten'.

Motivatie van medewerkers om te gaan melden
D: 'Ja, ja, kijk dat systeem geldt ook voor agressie en dat soort zaken en mensen kennen het systeem wel goed dus hoe je moet melden en er is op zich wel een redelijk grote meldingsbereidheid, maar ja ik weet natuurlijk niet wat mensen niet melden, dat weet ik ook niet. Maar ik kan me voorstellen dat met een datalek de drempel

wel wat hoger is. Laatst was iemand bijvoorbeeld een testrapport kwijtgeraakt als psycholoog tijdens een verhuizing was dus nog op papier, ja de doos moest van het ene naar het andere gebouw dat is netjes gebeurd, die doos is wel overgekomen alleen het rapport is in die tijd, er zat ook nog een vakantie tussenin, toen ze de doos uitpakte was het rapport weg. Ja, toen is ze een week lang is ze aan het zoeken geweest naar dat rapport totdat ze echt dat ja ik kan het echt niet vinden en toen is ze naar haar leidinggevende gegaan van ja ik ben het kwijt. En toen was die leidinggevende chagrijnig zo van ja waarom vertel je me dat nu pas een week nadat je dat geconstateerd hebt? Ja, anderzijds kan ik het me ook wel voorstellen want ja het is natuurlijk erg lullig dat het gebeurt dus je probeert natuurlijk alles in het werk te stellen om dat ding terug te vinden en dat je op een bepaald moment dan die drempel op gaat van ja ik moet het dan toch maar melden'.
Onderzoeker geeft aan dat het vergelijkbaar is met het verliezen van je portemonnee dat je dan ook eerst nog hoopt dat je hem terugvindt D antwoordt: 'Ja, deels lijkt het daar op, maar het is natuurlijk ook gênant om dat te moeten melden. Ik denk dat het ook gênant is: stel je voor je hebt toch gegevens naar je privéaccount verplaatst want je wilt thuis er nog aan werken, dat is op zich een oprechte reden en je computer of je laptop wordt gestolen of gehackt ja dan moet je denk ik wel even een drempel over om dat te zeggen, omdat je dan inderdaad ook toe moet geven dat je iets gedaan hebt wat niet mag. Dus dat blijft een moeilijkheid. Het zit natuurlijk wel als die gegevens op straat komen en blijkt dat je het dan wist en je hebt het niet gemeld dan heb je natuurlijk ook een probleem'.

Rol van de Autoriteit Persoonsgegevens
Onderzoeker vraagt of D wel eens iets van informatie heeft ontvangen van de AP D antwoordt: 'Nou nee dat is dus de hele droefheid ervan. Ja, dat vind ik wel, want het roept op dat je in een enorm bureaucratisch systeem terecht bent gekomen. Je hoort echt helemaal niets terug, niet eens een ontvangstbevestiging. Ja je moet het formuliertje invullen en dan staat er van u heeft het ingevuld, bedankt'.
D: 'Nee en ook niet van kans op onderzoek ofzo of wat dan ook. Een tijdje geleden hoorde ik ook dat ze vorig jaar 60.000 meldingen hadden gehad, ja daar kunnen ze natuurlijk ook helemaal niks mee'.
Onderzoeker geeft aan dat er volgens de AP nog maar rond de 4000 meldingen zijn gedaan dit jaar D antwoordt: 'Oh, nou dan heb ik een verkeerd getal. Maar dan nog ook op 4000, ja wat moeten ze ermee? En dan krijgen ze dat soort flutmeldingen die ik dan doe, waarvan ik ook denk ja daar willen ze ook helemaal niks mee denk ik'.
Onderzoeker vraagt hoe D tegen de rol van de AP aan kijkt, D antwoordt: 'Ja, ja, wat moet ik daarvan vinden? Kijk, als ik zelf denk ook waar volgens mij de regels op gedoeld zijn dat zijn meer de grotere incidenten en dat ze daar een rol in vervullen dat lijkt me heel goed, maar dit heeft niet zo heel veel effect op de kleinere incidenten dan denk ik van ja. Ik vind het ook lastig dat die regelgeving in die zin onduidelijk is. Aan de ene kant hele hoge boetes en aan de andere kant een onduidelijke regelgeving, ja…'
Onderzoeker vraagt aan D of D wel eens naar AP is toegestapt met vragen: 'Nee, ik volg meer de landelijke discussie hierover en als je kijkt GGZ-Nederland heeft wel zo'n website waar je onderling aan elkaar vragen kunt stellen. Ja, iedereen heeft die vraag wat moet je wel of niet melden? De meeste instellingen kiezen er dan maar voor om het zekere voor het onzekere te nemen, want op zich zo'n formuliertje invullen dat is het werk niet, een kwartiertje'.
Onderzoeker geeft aan dat de formulieren wel vrij uitgebreid zijn, D antwoordt: 'Nou ik vind het wel meevallen hoor. Het is toch van nou wat is er gebeurd en wat heb je vervolgens gedaan. De moeilijkheid in het systeem is dat je kunt een voorlopige melding doen, maar als je hem dan vervolgens weer oproept, moet je gewoon weer het hele formulier opnieuw invullen, je krijgt niet je oude formulier terug'.
Onderzoeker geeft aan dat ze ook nog geen boetes hebben uitgedeeld D antwoordt: 'Nee, en ze hebben het op een bepaald moment ook wel wat genuanceerd hè dat ze niet in één keer een factuur schrijven, maar dat ze waarschuwen'.
D: Ja, daarom. Maar in die zin, laatst hoorde ik iemand in een interview ook op de radio zeggen ja het wordt tijd dat er een keer een boete wordt uitgeschreven. Ja, ik denk, ja dat is een politiek middel dan.
D: 'Nou ja je loopt nu wel het risico dat omdat het zo fors gebracht is ook door marktpartijen van pas op die boetes, dat iedereen heeft even op scherp gestaan dat als er nu niets gebeurt, twee jaar lang ofzo, ja dan zakt het ook weer in, omdat organisaties zich daarop aanpassen. Er zijn natuurlijk veel meer toezichthouders en ja als je het idee hebt van ze zijn er wel maar ze doen toch niks. Wij moeten ook bij de AP melden welke persoonsgegevens wij verwerken en op welke plek nou dan heb ik eens even gekeken wat wij daar hebben staan dat is volgens mij van 20 jaar geleden ofzo, dat is enorm verouderd, maar daar gebeurt dus ook niets mee en dan kijk ik bij andere instellingen en dan wij hebben er nog vier of vijf dingen staan en anderen hebben er

maar één of twee dingen staan. Er is dus ook geen enkele controle vanuit de autoriteit om te zeggen van 'goh wat jullie daar hebben klopt dat wel?'
Onderzoeker geeft aan dat ze misschien ook geen capaciteit daarvoor hebben D antwoordt: 'Dat denk ik ook niet. Ik weet niet hoeveel mensen daar zitten'.

Voorbereiding op de Europese Verordening
D: 'Ja daar zijn we op dit moment wel hard mee bezig. Ik bedoel met die externe partij aan het kijken in hoeverre voldoen we daaraan, maar dat zit met name rond de bewustwording, toezicht en sanctiebeleid'.
D: 'Dat kwam dus uit die nulmeting en nu moeten we wat meer concreet gaan kijken van welke punten schieten we nu tekort en ja dan moet je gaan prioriteren waar je als eerste mee aan de slag gaat'.
Onderzoeker vraagt of die nulmeting in het begin van het jaar gedaan is D antwoordt: 'Nee, iets later, mei geloof ik'.
Onderzoeker en dat is toen gedaan en nu is eigenlijk stap 2 D antwoordt: 'Ja, dan ga je weer iets meer de diepte in dus nu gaan we iets meer kijken van goh waar moeten we nog een verbeterslag maken'.

6.5 Categorisatie interview zorginstelling E

Achtergrond van de Functionaris voor de gegevensbescherming
E: 'Ja, klopt. Ik werk sinds 2010 hier. Ik begon als senior systeembeheerder. Na 2 jaar ben ik ICT-architect geworden. Toen heb ik me beziggehouden met vooral de inrichting van het applicatie en informatielandschap. En ja dan dien je dus ook rekening te houden met allemaal kaders die er zijn en dat heeft automatisch ook een technisch karakter, maar ik ben altijd nieuwsgierig geweest. Zodoende kwam ik ook achter de Wet Meldplicht Datalekken en dat het eraan zat te komen en toen heb ik dat al besproken, onder de aandacht gebracht wat hogerop, dus bij de bestuursstaf en zodoende is eigenlijk vanuit de bestuursstaf de wens uitgesproken van waarom ga jij niet functionaris van de gegevensbescherming worden? Dus daar heb ik even over na moeten denken en toen gezegd van 'nou laten we dat maar doen'. De functie is nodig en het is goed als we hier een dergelijke functie hebben, dus laat ik hem maar gaan vervullen. Dus eigenlijk sinds begin dit jaar ben ik hier functionaris'.
E: 'Ja, sinds de wet in werking is getreden of eigenlijk sinds februari'.
E: 'Die volg ik. Een opleiding van twee jaar. Alle aspecten die bij een functie komen kijken die worden daar behandeld. Je hebt natuurlijk een stuk wetgeving, maar ook governance en ook de technische infrastructuur, maatregelen worden besproken, maar het wordt ook in perspectief van Europa gezet of als je eventueel met internationale ondernemingen gaat samenwerken. Een vrij brede opleiding vind ik en erg interessant'.

Thema in beeld bij bestuur
E: 'Nou ik heb in eerste instantie met de bestuursstaf gesproken en dat is eigenlijk via het informele circuit. Ik werk hier al een tijdje dus ik ken veel mensen, dus dan weet je gewoon voor dit onderwerp moet ik bij die zijn, dus ben ik gewoon maar even een kop koffie gaan drinken en ben ik gaan praten gewoon en dat is dus bij de bestuursstaf terechtgekomen en daar kwamen we tot de conclusie van ja dit moet niet een losstaand initiatief zijn het moet gedragen worden vanuit het bestuur alleen dan kun je er eigenlijk voor zorgen dat je voldoende maatregelen kunt treffen als organisatie. Het is niet alleen een technisch stuk, maar ook een organisatorisch stuk en je hebt daar gewoon het support en het mandaat ook wel van het bestuur voor nodig. Dus om je vraag te beantwoorden het bestuur die staat daar helemaal achter. Daar hebben we ook mee aan tafel gezeten en helemaal uitgelegd wat we willen.

Inrichting informatiebeveiligingsbeleid
Ik heb een plan van aanpak geschreven voor een periode van twee jaar waarin ik aangeef hoe we gaan werken aan het organiseren van gegevensbescherming binnen deze organisatie'.
Antwoord van E op vraag van de onderzoeker of het plan vanuit E beschreven werd en dan door het bestuur werd goedgekeurd: 'Ja, en dat is goedgekeurd door het bestuur. Onderdeel daarvan is dat de mensen van de bestuursstaf waarmee ik gesproken heb die zijn nu lid geworden van het zogenaamde p-team, het privacyteam. En zij zijn degene die de afhandeling doen van de meldingen die er komen maar ook die zich bezighouden met allerhande zaken die te maken hebben met privacy. Dus op het moment dat je, we zijn bijvoorbeeld nu bezig met het kijken naar een nieuw labsysteem, dat betekent dat er bloed geprikt gaat worden, dat betekent dus persoonsgegevens, bijzondere persoonsgegevens, dus dan moet je uitzoeken ja hoe zit dat dan met de

verantwoordelijkheid, wie is de bewerker, verwerker, een hele trits zaken en dat bespreken we met het p-team om te kijken in hoeverre er rondom dat onderwerp maatregelen nodig zijn'.
E: 'Ja, nou wat we nu aan het doen zijn is het inventariseren en het verzinnen van zinvolle stappen en dan in fase 2 gaan we dat expliciet uitvoeren en uitrollen en daar zijn we natuurlijk al mee bezig maar daar is fase 2 eigenlijk echt voor. In fase 3 dat heet reflectie en borgen dus dan gaan we het evalueren. Dus dan gaan we kijken van hoe is dat nu gedaan, moeten we het aanpassen of bijstellen?'

Meldingen
E: 'We hebben nu iets van vijf meldingen gedaan bij de Autoriteit.

Evaluatie van incidenten
Zoals wij het zien, zijn het steeds leermomenten 'never waste a good crisis'. Dus we gebruiken het om alerter te worden en om te ontdekken waar bijvoorbeeld zwakke plekken zitten in bijvoorbeeld onze infrastructuur en dat kan leiden tot een advies van 'joh we moeten het anders gaan doen'.

Voorbeeld van incident
Een voorbeeld daarvan is dat we nu 17 meldingen hebben gehad op het gebied van cliëntendossiers die bij printers liggen, dus bij printers in de gang en we hebben natuurlijk getoetst van hoe kan dat nou dat dat gebeurt want we hebben toch de mogelijkheid om beveiligd te printen, dus dat mensen naar hun mailbox printen en dan moeten mensen naar de printer lopen en daar hun mailbox openen en dan kiezen van stuur het er nu maar uit. Maar ze kunnen kiezen om dat niet te doen, ze kunnen kiezen om dat niet standaard te maken en dat gebeurt en dan is het de vraag van 'goh hoe breng je dat nu onder de aandacht van 1800 medewerkers?' En die 1800 medewerkers die worden allemaal op de nek gezeten om patiëntgebonden tijd te besteden, het is echt een beetje een soort van crisistijd in de zorg, dus ik kan niet met een pak papier aankomen en zeggen hier heb ik helemaal beschreven wat je allemaal moet doen, hier heb je dat lees dat maar eens. Daar hebben de mensen geen tijd voor'.

Procedure Meldplicht Datalekken
Antwoord van E op vraag van de onderzoeker hoe het protocol is ingericht (Onderzoeker laat ondertussen protocol zien op PC-scherm): 'Als het goed is had ik hem namelijk al klaar gezet. Ik dacht jij gaat dat soort dingen wel willen zien. Dit is het protocol en dit is ons kwaliteitssysteem en dan een stukje inleiding, wat is een datalek, wat voorbeelden een soort beslisboom van: wanneer moet er nou daadwerkelijk gemeld worden aan de autoriteit. Wie gaat hierover? Wie speelt hier een rol over? Dat is het p-team die bovenste ben ik. Nou wat moet je doen: Meld het direct via dit e-mailadres, informeer je leidinggevenden doe een veiligheidsmelding, dat is het VIM'.
E: 'En dan gaat het privacyteam aan de slag en nog meer en nog meer en ook met de lijnorganisatie als er nog vragen zijn natuurlijk'.
Onderzoeker vraagt of er ook teruggekoppeld wordt aan de medewerker E antwoordt: 'Ja, zeker. Dat is erg afhankelijk ook wel van de aard van de melding. Sommige dingen zijn toch wel heel erg stom. Er is een locatie zeg maar waar de medewerkers het niet tussen de oren krijgen dat ze naar beveiligde docs moeten printen en daar krijgen we vaak meldingen van cliëntgegevens die op de printer liggen'.
Onderzoeker vraagt zich af hoe het dan komt dat deze medewerkers wel melden E antwoordt: 'Zij melden het niet. Iemand, een kwaliteitsadviseur die verbonden is aan dat centrum. Die doet tegenwoordig zo'n ronde om te kijken van vis ik daar nou nog wat op? En ja hoor: en dan maakt hij een melding en dan hangen wij aan de telefoon met degene die dat geprint heeft om te zeggen van ja dat moet je niet doen. En dat werkt niet, dus we doen het ook aan zijn leidinggevende dat zeggen we ook en de teammanager en we hebben het inmiddels ook doorgesluisd naar de algemeen directeur van dat centrum. En het staat nu ook in de jaarrapportage in de kwartaalrapportage van mij aan het bestuur van nou dit is een issue. Een niet uit zichzelf te corrigeren issue zeg maar. Dus mijn advies daarop is om te starten met een proefconcept voor follow-me printen. En het idee daarachter is van mensen hebben maar één printer en kunnen niet meer kiezen'.
E: 'Relatief simpel te implementeren vonden wij'.
Onderzoeker geeft aan dat je dan wel het probleem blijft houden dat mensen het naar hun thuismailadres kunnen sturen om daar te printen E antwoordt: 'Ja, maar oké. Maar als je gaat analyseren welke lekken er allemaal zouden kunnen gebeuren, dat krijg je nooit allemaal gedicht. Dus ik vind het logisch dat mensen proberen te printen en dat is voor hun werk is dat verklaarbaar en dan moet je dat faciliteren op een zo veilig

mogelijke manier. En op het moment dat we dat hebben gedaan dan hebben we dus meer dan vijftig procent van onze datalekmeldingen die hebben we dan afgedekt'.
E: 'En als dan blijkt dat mensen persoonsgegevens meenemen naar huis. Ik kijk niet in mailboxen dat kan ik niet en dat mag ik niet. We hebben daar wel gedragsregels over afgesproken met elkaar maar ja als daar een incident uit voortkomt dan gaan we daar wel weer op acteren'.
Antwoord van E op vraag van de onderzoeker of meldingen afgehandeld worden bij het bestuur: 'Nou de bestuursstaf. Het bestuur zelf zal niks doen met de meldingen. Wat we hebben gedaan. We hebben een protocol opgesteld, een protocol Meldplicht Datalekken en dat hebben we gecommuniceerd aan de hele organisatie, dat brengen we met regelmaat onder de aandacht. En daarin staat eigenlijk van nou wat moet je doen als je een issue hebt waarvan je denkt 'goh daar zouden wel eens persoonsgegevens bij betrokken kunnen zijn'. Bijvoorbeeld ik mail een cliënt om die uit te nodigen om te komen praten en je komt erachter dat je de mail naar de verkeerde persoon hebt gestuurd, oeps. Nou dan moet je dus gaan melden, en dan bedoelen we melding intern he, dus bij het p-team. En dan gaat het p-team die gaat aan de slag met die mensen en met mij ook van 'goh is er sprake van een datalek of niet?' Nou dat gaan we dan uitzoeken en daar betrekken we eventueel ook de lijn bij en het bestuur komt daar niet bij kijken'.
Antwoord van E op de vraag of er als er sprake is van een datalek wel overleg plaatsvindt met het bestuur: 'Nee, niet perse laat ik het zo zeggen'.

Communicatie-inzet naar aanleiding van Meldplicht Datalekken
Antwoord van E op vraag van de onderzoeker of medewerkers protocol via het systeem kunnen vinden: 'Ja, ze kunnen via intranet zoeken, ze kunnen het nieuwsbladbericht erbij pakken als ze die nog weten te vinden, ze kunnen via het kwaliteitssysteem en daar wordt iedereen in getraind, iedere nieuwe medewerker krijgt een training dan kunnen ze het via het kwaliteitssysteem opzoeken. En op het moment dat zeg maar die intranetpagina er is, dan staan daar ook allerhande makkelijke links zodat ze dat ook makkelijk weten te vinden'.
Antwoord van E op vraag hoe het protocol onder de aandacht is gebracht: E: 'Nou we hebben twee manieren waarop je standaard kunt communiceren met medewerkers en dat is het intranet en daar hebben we een berichtje op gezet. Als mensen inloggen dan starten ze meteen op met de nieuwspagina van het intranet, ze krijgen meteen dus nieuws te zien. De bevinding is wel dat dat eigenlijk nooit gelezen wordt, dat wordt meteen weggeklikt. Maar goed het is een manier om te communiceren dat is één kant en we hebben een maandelijkse uitgave van ons nieuwsblad en daar staan dan zaken in en dat wordt wel gelezen en daarin hebben we dat ook onder de aandacht gebracht. We hebben een kwaliteitssysteem waarin al onze kwaliteitsdocumenten staan en daar is dit één van dus mensen kunnen het altijd vinden. We hebben daar ook wel vrij veel reacties op gehad, dus we hebben wel het gevoel van 'hee het is gelezen. Mensen hebben er wat meegedaan''.
E: 'Ja, we kregen een toename van meldingen en dat is goed. En je zou denken van nee dat is niet goed, maar dat is juist goed. Zo zien we dat in ieder geval'.
E: 'Maar dat is één kant van de zaak. Een ander ding waarvan we dachten het is redelijk passief hè je informeert ze en dan hoop je maar dat mensen het lezen en dan is intranet niet handig merken we. Ons nieuwsblad is handiger, maar het is nog steeds passief want we hebben nu een paar maanden terug hebben we dat in ons nieuwsblad gezet, maar nu staat het niet in ons nieuwsblad en nu leest men dat niet, dus hoe blijft dat leven? Dus wat we gedacht hebben en dat is naar voorbeeld van een andere zorginstelling. Ik heb met de functionaris gegevensbescherming daar gepraat en we hebben hun idee overgenomen. We hebben stellingen ontwikkeld, simpele stellingen. Even denken nou ja bij wijze van spreken je wilt een uitdraai van een cliëntendossier maken wat doe je? En dan vier opties ofzo: je print het naar de printer, of je print het via beveiligde mailbox of je stuurt het naar je mail en je print het thuis. En die stellingen met antwoorden die sturen we naar alle teammanagers, zodat het meegenomen kan worden in het wekelijks of tweewekelijks of maandelijks teamoverleg: één stelling per keer per team. Dus roep maar wat denk jij en wat denk jij en wat denk jij en er is geen goed antwoord of slecht antwoord in die zin daar gaat het niet om het gaat er wel om dat mensen leren na te denken van 'hee kan ik dat nou zomaar op mijn bureau laten liggen of niet''.
Onderzoeker vraagt wie er dan bijvoorbeeld bij zo'n teamoverleg zitten E antwoordt: 'Nou de behandelteams bijvoorbeeld. Ook de mensen die de wijk ingaan die hebben elke ochtend een start en die hebben dus een teammanager en die hebben dus een plek waar ze dan overleggen en vanuit die agenda vanuit de bestuursstaf wordt dan gezegd van jongens je moet dat onderwerp op de agenda zetten en dat is nog niet uitontwikkeld. De manier waarop we het willen doen is, we zijn ook aan het werken aan een eigen pagina van een eigen stukje op het intranet en dan is het idee dus dat je de stelling van de week krijgt en dat je die stelling bespreken ze en op

het intranet staat dan voor de stelling van de week een soort toelichting en wel hierom is het handig dat je die persoonsgegevens niet openlijk laat liggen en dan volgende week is het weer een ander verhaal, maar die uitwerking die moeten we nog schrijven'.
E: 'Dat is onderdeel van het plan van aanpak'.

Maatregelen bij niet naleven regels
E: 'Nou ja er zitten nog geen consequenties aan verbonden voor het personeel. Er zijn een aantal dingen te bedenken waar dan wel consequenties aan te verbonden zijn. Kijk de printer in kwestie staat in een afgesloten ruimte die alleen maar toegankelijk is voor personeel, maar huishoudelijk personeel komt er niet bijvoorbeeld en cliënten al helemaal niet. Dus dat is dan geen grond om te zeggen van het komt in je beoordelingsgesprek terug'.
Onderzoeker vraagt of E controle heeft over het EPD-systeem en of E kan zien wie daar wanneer in is geweest E antwoordt: 'Ja, dat is in te zien. Ik niet, ik kan dat niet zien, dat wil ik ook niet. Er is een soort procedure voor dat de zorgadministratie met een leidinggevende daar wel eens met zijn tweeën naar kijken. Daar moet dan een grond voor zijn'.
E: 'Nee, ik bemoei me daarmee in de zin van: ik moet weten dat dat kan ik wil weten dat dat netjes gebeurt dus als ik dat weet dan ben ik blij. Ik weet dat bijvoorbeeld in een van de afhandelingen van zo'n melding is het noodzakelijk gebleken om daar naar te gaan kijken zo van 'goh heeft die persoon dan toegang gehad tot het cliëntendossier of wat hoe zat dat?''

Rol van de Autoriteit Persoonsgegevens
E: 'Uhm, nou de autoriteit is voor mij op dit moment nog wel een beetje een onduidelijke entiteit als zodanig en ik weet wat hun bevoegdheden en hun rol is maar ik heb niet met ze te maken gehad nog. Ik ben wel geregistreerd bij hen als zijnde FG. Dus wij hoeven bij hen geen meldingen te doen over onze bewerkingen dat kan ik zelf dan bijhouden en dat hou ik ook bij. Ik ga ze binnenkort benaderen met een vraagstuk. Ik verwacht dat ik hen daarvoor mag benaderen en ja ik weet het niet. Het is een onbekende eenheid, een grootheid, ik heb nooit met ze te maken'.
Onderzoeker vraagt of E geen contact met de AP heeft gehad E antwoordt: 'Nee, nee ook geen reden toe gezien zeg maar.
Onderzoeker vraagt of E nog iets heeft teruggezien van de meldingen die E gedaan heeft E antwoordt: 'Nee, nee. En kijk in het begin was het heel lastig hè waren ze helemaal understaffed. Dus toen kregen we bijvoorbeeld geen registratie terug van meldingen. En dan moest je bellen van ik heb net een melding gedaan maar ik weet de code niet en dan krijg je een student aan de telefoon en ja die wist het ook niet dus dat is niet handig. En later is dat meer op orde gekomen. Ik verwacht ook niet dat zij daarover terugkomen. In ieder geval niet gezien de aard van de meldingen die wij gedaan hebben dat is allemaal zo kleinschalig eigenlijk daar wijst niet uit dat er een grove nalatigheid is aan onze kant ofzo. Dat is niet om ons op de borst te slaan, maar we hebben gewoon denk ik de bescherming wel aardig op orde, dus gelukkig hebben we nog niet gek veel ernstige dingen meegemaakt'.
Antwoord van E op vraag van onderzoeker of ze informatie van AP hebben gehad toen de Meldplicht inging E antwoordt: 'Uhm, even denken nou ik weet dat er informatie beschikbaar was via de website van de autoriteit, maar hier heb ik zeg maar vanaf het moment dat het onderwerp bij mij op de radar kwam heb ik dat in de gaten gehouden en ben ik gaan lezen en uit zitten pluizen. Ik geloof dat er een brief is geweest van de autoriteit aan alle GGZ-instellingen, maar die is verstuurd naar de bestuurder, die heb ik niet gekregen, omdat ik ook toen nog geen FG was volgens mij'.

Voorbereiding op de AVG
Onderzoeker vraagt aan E of dat plan van aanpak voor de komende twee jaar geschreven is om voorbereid te zijn op de Europese Verordening E antwoordt: 'Dat houdt er rekening mee ja en dat is best een klus. Mijn redenering was eigenlijk van ja we doen een hoop dingen al goed maar ook een hele hoop dingen echt niet. En als ik nu kijk naar hoe iedereen nu knel zit in zijn tijd en knel zit in zijn budget ja hoe sterk pak je uit met je maatregelen? Dus ik had eigenlijk het idee van nou we moeten stapsgewijs, gefaseerd toewerken naar het verhogen van je bescherming en dat betekent ook sec genomen zijn er een aantal verplichtingen waar we op dit moment echt niet aan voldoen en zeker als straks die Europese Verordening tot kracht wordt, als die straks gehandhaafd gaat worden dan hebben we een uitdaging omdat je dan met je accountability zit. Bijvoorbeeld Data interoperabiliteit ook zo'n mooie maatregel. Maar accountability dat betekent: je moet kunnen laten zien

dat je doet wat je doet en wat je doet en niet alleen maar zeggen van ik heb een informatiebeveiligingsbeleid maar je moet echt zeggen ik heb dit gedaan en je moet de werking ervan kunnen aantonen maar ook op 26 februari 2017 moet je ook kunnen laten zien van toen werkte het ook en als je nu kijkt naar de verschillende gegevensverwerkingen die we kennen heb ik er 38 kunnen identificeren. Voor veel daarvan geldt dat we geen dergelijke accountability hebben dat hebben we niet in place. Dat kost tijd om dat goed op te tuigen en dat kost ook geld. Sommige systemen die zijn bijvoorbeeld gebouwd door een paar enthousiastelingen, door hele professionele enthousiastelingen maar daar is accountability niet aan de orde geweest, dus hoe ga je dat inrichten dan? Dus daarom trapsgewijs moeten wij steeds volwassener worden.
Antwoord van E op vraag van onderzoeker in hoeverre E denkt dat ze voorbereid gaan zijn in mei 2018: 'Nou ik denk dat we het goed op gang krijgen. We hebben de gegevensverwerkingen in kaart, we zijn de bewaartermijnen in kaart aan het brengen. Dat betekent dus ook dat je intern moet afspreken over van wanneer ga je dingen vernietigen want je mag het niet langer bewaren dan strikt noodzakelijk. Ik denk dat we op 80% zitten, laat ik het zo zeggen. Want die overige 20% dat zit hem vrees ik in bestaande systemen zoals ons EPD. Data interoperabiliteit is ook zo'n ding uit de Europese Privacy Verordening en ja dat is een complex verhaal. Je bent verplicht om mensen in een elektronisch leesbaar formaat gegevens mee te geven als ze vertrekken naar een andere partij. Nou de letter genomen kun je dan gewoon een dump maken van je hele database in XML-formaat en dat geven en succes. Maar dat werkt niet mensen hebben daar niks aan. Mensen kunnen daarmee niet naar een andere GGZ gaan en zeggen van hier heb je mijn dossier. Het is technisch leesbaar maar het is betekenisloos. Dus je moet zien te komen op dat niveau tot een soort marktstandaard van gegevensuitwisseling'.
E: 'Dat zit niet in het EPD verwerkt en dat is ook lastig want we hebben een EPD van organisatie A, maar als iemand verhuist dan komen ze bij een GGZ die gebruik maakt van een EPD van organisatie B. En dat is een andere opzet. Dus de informatie in het systeem van organisatie A is misschien niet leesbaar voor organisatie B'.
E: 'En is het nu onze plicht om te zorgen dat organisatie A en organisatie B met elkaar om tafel gaan zitten? Is dat de geest van de wet? Is dat de letter van de wet? Op dat punt zijn we in ieder geval absoluut nog niet klaar'.
E: 'Nou weet je wat het is voor nieuwe systemen zal gaan gelden dat we dat dus gaan uitvragen. Dus als er een nieuw salarisverwerkingssysteem ofzo komt als dat soort systemen nu aangeschaft moeten gaan worden dan zeggen we tegen zo'n leverancier laat maar zien dat jij dat kan, accountability. En dan is dus het advies in de richting van de Raad van Bestuur als ze dat niet kunnen aantonen dan mag je er niet mee in zee gaan, want EPV. En dan kan dus nog steeds de Raad van Bestuur besluiten van ja gezien de huidige stand der techniek, zien wij geen alternatief in de markt om zo'n salarisverwerkingssysteem aan te schaffen. Nou dan vind ik dan zijn we weer 100%. Dan kan je zeggen van ja leuk dat je dat zegt, de elektronische uitwisseling, maar daar is de markt niet klaar voor en dat is niet ons pakkie aan zeg maar'.
E: 'Dus ik denk ja, dat we 80% klaar zijn'. Onderzoeker vraagt of E op dit moment bedoeld of dan E antwoordt: 'Nee, dan. Op dit moment moeten we echt nog veel verder de plaatjes inkleuren van de verwerkingen die we hebben. Ik vind dat we voor awareness dat vind ik echt een speerpunt van mijn plan van aanpak dat moet vele malen hoger zijn dan dat het nu is het moet een soort in de genen komen te zitten dus ja we moeten voorlopig nog wel even de komende anderhalf jaar blijven communiceren dus daar hebben we dat plan voor'.

Samenwerking met communicatieafdeling
Antwoord van E op vraag van onderzoeker of communicatieafdeling wordt meegenomen in plan van aanpak: 'Ja, ik heb hier het plan van aanpak. Inleiding, meldplicht datalekken, het juridisch kader, het doel van het plan van aanpak, de samenwerking met een p-team, nou een collega is onderdeel van het p-team die draagt zorg voor communicatie. Nou in fase 1, dus ik heb het even opgedeeld in vier fasen. Eerst inventariseren en alles in kaart brengen en dan maatregelen verzinnen om compliant te zijn. In de eerste fase hebben we hier voor communicatie: dat er een protocol wordt opgesteld, dat die wordt gedeeld via het kwaliteitssysteem en in het nieuwsblad in samenwerking met de afdeling communicatie wordt een communicatieplan opgesteld en dat gaan we dan in uitvoering brengen: regelmatig terugkerende korte presentaties in teamoverleggen, privacy standaard op de agenda, maken en verspreiden van flyers zoiets als dat (wijst naar 'ZEKER' campagnemateriaal) en regelmatige berichtgeving op intranet. Dus met de afdeling communicatie hebben we nu iets van drie keer gezeten om een soort van communicatieplan op te stellen. Dat hebben ze ook gemaakt en we hebben dus ook gedacht van ik was met wat directeuren aan het praten en we hebben een beetje ons hoofd zitten breken van nou hoe bereik je nou mensen? Zeg maar behandelaren die lezen het intranet niet die hebben daar geen tijd voor, het nieuwsblad wel. Maar we hebben van die prachtige koffieautomaten met een digitaal display en als je

die even niet gebruikt dan gaat hij op screensaver en dan krijg je een mooi plaatje van koffiebonen enzo. Ik had zoiets van maak dat plaatje nou een plaatje van privacy, dat mensen dus bij wijze van spreken een leuk plaatje met een cartoonpoppetje met wees geen datalek ofzo. Iedereen gaat koffie halen en dan zien ze dat. Onderdeel van het communicatieplan. Daar zitten kosten aan verbonden, want dat moet gemaakt en geïmplementeerd worden. Dat moet met usb-sticks op die koffiezetapparaten gezet worden'.

Evalueren van beleid
Antwoord van E op vraag van onderzoeker of er op dit moment een beeld is van hoe de awareness of beveiligingsmaatregelen zijn in de instelling: 'Ja, dat laatste wel. Awareness is lastig te kwantificeren. Je kunt er wel een indicator voor verzinnen in de zin van hoe vaak wordt er nu een melding gedaan, dat kun je meten. En voor de beveiligingsmaatregelen daar zie je toch, want ik ben een privacyhuishouding aan het voeren dus ik registreer al dat soort zaken. En wat we dus ook doen is als je alle maatregelen wilt nemen die je kunt nemen om compliant te worden dan heb je een portemonnee nodig dus ik vind dat niet reëel dus daarom doen we dan ook een risicoanalyse op elk systeem dus dat is ook een bewijs dat we een privacy impact assessment uitvoeren en daarin zit dus van ja welke maatregelen hebben we al wat is de aard van die gegevens? Hoe spannend is dat? Wat is nou het risico dat daar een datalek in gaat ontstaan? En aan de hand daarvan hebben we een lijst met de huidige maatregelen en ook een rationele afweging van waarom je dan iets kiest of niet kiest'.
Onderzoeker geeft aan dat de privacy impact assessment toch best uitgebreid is of ze een nulmeting doen E antwoordt: 'Nou dat hangt ervan af, je kunt het zo uitgebreid en zo breed maken als je het zelf wilt'.
E: 'Nogmaals dat hangt ervan af hoe je het insteekt. We hebben nu nog niet echt een standaard PIA. Er is een PIA van NOREA. Dat is een bedrijf die dat heeft opgesteld en die is goed bruikbaar, maar die richt zich meer op de informatiebeveiliging dan op compliancy naar de Wet Bescherming Persoonsgegevens of de EPV. Kijk ik heb zelf zoiets van we moeten een privacyhuishouding houden en daarin zegt de wet of zegt de autoriteit persoonsgegevens van we willen een aantal dingen daarover weten en die kan ik toetsen. Bij het nieuwe labsysteem bijvoorbeeld ben ik dus eigenlijk die lijst aan het invullen van wat de Autoriteit Persoonsgegevens van een verwerking zou willen weten, dus wie is de verantwoordelijke, wie zijn de betrokkenen, welke gegevenscategorieën ken je, zijn er bijzondere persoonsgegevens wat is de grondslag wat is het doel waarvoor je ze gebruikt. Dat zijn er zes en welke maatregelen heb je genomen en zijn die afdoende dat is de risicoanalyse. Dan heb je acht vragen gesteld en dan heb je eigenlijk al een basis PIA te pakken wat mij betreft en die kun je tot in detail uitwerken, maar daar heb je meestal geen tijd voor en ik vind dat niet noodzakelijk voor sommigen wel. Soms dan is het complex'.

Bekendheid 'ZEKER' campagne
Onderzoeker vraagt of E bekend is met de 'ZEKER' campagne van de NVZ, E wijst naar een doos en antwoordt: 'Ja, die gaan we ophangen in november, dat is het al dus'.
Onderzoeker vraagt of E ook meedeed aan die online quiz E antwoordt: 'Ja, hebben we ook mee geadverteerd ook op het intranet en in het nieuwsblad en daar hebben van de 1800 medewerkers wel 40 aan meegedaan'.
Onderzoeker vraagt wat E van de campagne vond E antwoordt: 'Ik vond het wel leuk, het was ludiek hè. Wat ik heel leuk vond was dat het niet het zwerende vingertje was. Mensen zien iets grappigs een beetje slepen en klikken. Je ziet zo'n buisje met water vullen van hoever je bent met je vragen en het kost niet zoveel tijd en het is toegankelijk, dus leuk als onderdeel van het totaalplan vooral heel goed denk ik. Ik blijf toch wel op de mening toegedaan dat je moet blijven herhalen. Anders dan gaat het niet leven. Het is niet iets, het is helemaal geen populair onderwerp, het is niet sexy het spreekt niet tot de verbeelding'.

Risico's van een datalek voor instelling
E: 'Ja, nou dan heb je het alleen maar over de gevolgen voor de instelling. Ik vind het belangrijker nog dat de doelgroep van ons die is bijna per definitie zwakker zou ik maar zeggen he dus ja wij behandelen jongeren bijvoorbeeld ook en mensen met een psychische aandoening mensen met geen goed verweer, dus die moet je goed beschermen. Als de behandelgegevens, dat zijn onze kroonjuwelen als die op straat komen te liggen, dan vertrouwt een client ons niet meer en dan heeft die client mogelijk echt wel grote persoonlijke schade. Dus dat is een ding, dat is voor ons zeer zwaarwegend. Qua instelling hebben we reputatieschade. We willen niet in het nieuws komen dat er dossiers van clienten op straat komen. Ja, kijk een ander gevolg is natuurlijk op het moment dat je dan een bezoek krijgt van de AP en ze vinden dat je op een bepaald punt grof nalatig bent geweest, verwijtbaar nalatig en je krijgt een boete nou ja die zijn enorm fors en dat wordt met de Europese

Privacy Verordening vele malen forser, dus dat kunnen we ook niet hebben, dat trekken we niet. Dus we moeten er echt alles aan doen om dat te voorkomen'.

Risico's in beeld bij het bestuur
Op de vraag of de gevolgen ook in beeld zijn bij het bestuur antwoordt E: 'Ja, ja'.
Onderzoeker vraagt of het voldoende aandacht krijgt E antwoordt: 'Ja, het mooie is natuurlijk dat de boete is hoofdelijk, dus de boete waarvoor onze bestuurder eigenlijk aansprakelijk is. En het kostte twee zinnen in een mailtje: 'Jij gaat die boete betalen, wat wil je dat we gaan doen? En die boete is 820.000 euro per keer''.
E: 'Ja, tuurlijk. Ik ben er wel voorzichtig mee geweest met bespreken omdat ik er zelf een hekel aan heb en dat zie je nu veel gebeuren dat die datalekken daar springen heel veel leveranciers op dat onderwerp en die hebben zoiets van wij hebben een product en daarmee raak jij in control en als ze dat nou zouden zeggen dan zou ik het nog oké vinden maar wat ze zeggen is: 'Weet jij wel dat jij 820.000 euro boete kunt krijgen? En dat is vreselijk, je gaat failliet'. En dat is een soort insteek op basis van angst waarvan ik denk 'ja dahaag, we moeten het goed regelen''.

Bijdrage van communicatie om risico's in te perken
E: 'Nou kijk, ik vind je hebt een aantal plichten als organisatie om je aan te houden: dat je je gegevens goed beveiligd en dat je maatregelen neemt technisch en organisatorisch om ervoor te zorgen dat er geen datalek ontstaat, maar wat wel gebeurt. Ja, dat kan gebeuren en dan moet je je best doen om dat te voorkomen of om schade in te perken en je moet de mensen erover inlichten en je moet er als organisatie van leren en je moet het de volgende keer beter doen. Onze portemonnee is niet groot genoeg om alle maatregelen te nemen die je zou kunnen nemen om dat beveiligingsniveau omhoog te brengen, dus de communicatie is heel belangrijk in hoe je hiermee omgaat als organisatie vind ik. De manier waarop we dat doen is dus door veel de hort op te gaan door veel het onderwerp te bespreken, bewustwording proberen te kweken door bijvoorbeeld die stellingen en dat onder de aandacht te brengen, mensen snel terugkoppeling te geven. Bijvoorbeeld er was een incident waarbij een medewerkster een foutmelding op haar scherm kreeg en ze drukte op printscreen en stuurde de hele printscreen naar de helpdesk en onze helpdesk is geoutsourcet dus dat is een ander bedrijf. En zij hebben wel een geheimhoudingsplicht ondertekend, maar op het scherm stonden ook nog patiëntgegevens open. Het elektronisch patiëntendossier stond daarachter en dan denk ik ja dat hebben ze niet nodig om te weten dat zijn persoonsgegevens daar moet je alert op zijn. Dus we hebben meteen contact gezocht met degene die dat meldde en gezegd van wat goed dat je het meldt want dat is het denk ik ook je moet mensen wel een soort van belonen dat ze hun best doen. Toen hebben wij ook contact opgenomen met de helpdesk van 'joh wees je ervan bewust dat als jij een melding krijgt: eigenlijk moet jij zeggen ik wil helemaal niks weten van patiëntgegevens of persoonsgegevens want dat heb ik helemaal niet nodig voor de uitvoering van mijn werk. Nee, ik moet een storing kunnen analyseren dus ik wil een foutboodschap ofzo maar verder niet'. Dus ook aan hun kant heb ik dat goed uit zitten leggen van 'joh wees je daarvan bewust'. Ik weet bijvoorbeeld dat de leverancier van ons EPD hun helpdesk is daar heel expliciet in die zijn daar goed in getraind. Die geven ook echt aan aan melders van 'joh deze informatie hoeven we niet te hebben, die willen we niet hebben dat moet je bij je houden'. En dan ben je denk ik goed bezig. En dat stuk communicatie, je moet het onder de aandacht blijven brengen. Ik blijf herhalen'.

Bereiken van de verschillende groepen
E: 'Nou wij hebben wel een standaard infrastructuur, een standaard werkomgeving, dus dat verschilt niet van groep tot groep. Iedereen komt op dezelfde manier op het systeem en krijgt daardoor dus eigenlijk toegang tot dezelfde communicatie'.
E: 'Nou huishoudelijke hulp zodanig als die mevrouw die hier net met de stofzuiger bezig was niet, die heeft geen werkplek als zodanig, die heeft niet de noodzaak om zich bezig te houden met de infrastructuur'.
Onderzoeker vraagt nogmaals naar de medewerkers die op locatie zorg verlenen: 'O ja, maar dan hebben ze een laptop van de zaak en die laptop van de zaak, die sluist hen automatisch door naar dezelfde omgeving'.
Onderzoeker vraagt of er wel een plek is waar ze kunnen werken E antwoordt: 'Ja, dat kan ook en nogmaals als zij dus bij een cliënt op bezoek zijn dan zitten ze met hun laptop bij de cliënt en die laptop is dan verbonden met ons systeem, dus dan zien zij ook weer het intranet als zij opstarten en dan ook in hun mail krijgen ze het nieuwsblad'.

Veranderingen sinds Wet Meldplicht Datalekken

E: 'Nou ik heb niet echt nog gegevens om dat te vergelijken. Ik zie natuurlijk wel het feit dat er gemeld wordt. Er wordt gemeld met een redelijke hoeveelheid maar ik denk dat dat meer zou mogen zijn en voorheen ja kijk de geheimhoudingsplicht, de medische geheimhoudingsplicht zit bij veel mensen goed tussen de oren dus er zit al een groot gevoel van awareness van cliëntgegevens mag je niet zomaar delen. Ik kan nog niet echt zien dat de bewustwording hoger is geworden ofzo'.

6.6 Categorisatie interview zorginstelling F

De functie van Functionaris voor de Gegevensbescherming

F is in november 2009 benoemd als security officer en houdt zich vanuit die functie bezig met informatiebeveiliging. Informatiebeveiliging heeft drie kenmerken: beschikbaarheid, betrouwbaarheid en vertrouwelijkheid. Sinds maart 2010 is F daarnaast privacy functionaris. De functie van FG is sinds 2013 ook belegd bij het College Bescherming van de Persoonsgegevens. F's hoofdtaak is security officer en de andere twee rollen doet F ernaast. F is verantwoordelijk voor al het beleid omtrent informatiebeveiliging. Daarnaast doet F bewustwordingscampagnes, geeft F voorlichting en adviseert F gevraagd en ongevraagd. Daarbij beweegt F zich door de hele organisatie, dus vanaf de werkvloer tot aan de Raad van Bestuur.

Awareness vergroten

F is verantwoordelijk voor de bewustwordingscampagnes, maar betrekt er wel andere mensen bij van bijvoorbeeld de communicatieafdeling. In 2011 is bijvoorbeeld een campagne gelanceerd waarbij door de hele instelling 300 gele vogeltjes zijn opgeplakt, zonder dat daar verder enige vorm van communicatie over is gedaan. Een week later zijn de vogels weer weggehaald en tot de maandag daarop is hier niks over gecommuniceerd. Mensen in de organisatie haakten op de campagne in door vogelgeluiden als achtergrondgeluid in te stellen. Het idee achter deze campagne was dat er juist reuring moest gaan ontstaan en dat mensen zich af gingen vragen wat die vogeltjes daar deden. De week erop is een poster verspreid met een geanonimiseerde dokter daarop. Je zag deze dokter een gesprek voeren per telefoon door de galerij waar in principe andere mensen dit gesprek konden horen. Op de poster stond een balustrade met daarop het kleine gele vogeltje. Deze werd ingezet als luistervink met de centrale boodschap: we hebben hier een luistervink en voor je het weet luistert of kijkt deze mee. Deze luistervink wordt ingezet als symbool voor informatiebeveiliging.
F komt nog voldoende mensen tegen die getraind moeten worden in het herkennen van phishingmails. Een mooi voorbeeld als onderdeel van de bewustwording was een bericht op intranet over ransomware. Vlak na dit bericht heeft zorginstelling F een phishingmail uit laten gaan. Als je goed naar deze mail keek zag je dat de afzender niet de stafdienst ICT was en als je goed naar de link keek zag je dat dat ook geen zuivere koffie was. Toch hadden best veel mensen op deze mail geklikt. Zo'n bewustwordingscampagne in de vorm van zo'n mail helpt alleen al om mensen scherp te maken.
Zorginstelling F kiest een paar momenten per jaar uit voor een bewustwordingscampagne. De ene keer pakken ze het iets groter aan dan de andere keer.

Communicatie-inzet informatiebeveiligingsbeleid

Normaal gesproken houdt F een presentatie voor nieuwe medewerkers waarin F aangeeft wat de instelling van nieuwe medewerkers verwacht. Nu is er net een film gemaakt voor nieuwe medewerkers die de eerst volgende bijeenkomst wordt laten zien. Ook gaat F bij de afdelingen langs en doet F presentaties over informatiebeveiliging, privacy en de Meldplicht Datalekken.
Zorginstelling F is al zes jaar aan de slag met communiceren rondom informatiebeveiliging. Het is ieder jaar een terugkerend thema. De evaluatie van de communicatie zou nog wel wat beter kunnen. F doet wel evaluatie met mensen die betrokken zijn geweest bij een bespreking en vraagt dan wel wat de betrokkenen goed en minder goed vonden werken, maar zorginstelling F vraagt de medewerkers niet specifiek om mee te evalueren. Na presentaties vraagt F ook wel om tips.

Thema in beeld bij bestuur

Ideeën over dit thema komen over het algemeen bij F vandaan. Toen bijvoorbeeld de Wet Meldplicht Datalekken werd ingevoerd heeft F een document opgesteld en deze aan de Raad van Bestuur gegeven met daarbij de opmerking: 'volgens mij moeten we dit en dit gaan doen'. Soms komt het ook bij de Raad van Bestuur vandaan als zij iets signaleren of een vraag binnenkrijgen. Het is dus tweerichtingsverkeer.

Verhouding tussen privacy en de bescherming van persoonsgegevens
Er wordt geen onderscheid gemaakt tussen privacy en de bescherming van persoonsgegevens bij zorginstelling F. F vindt privacy wel een redelijk containerbegrip, waar de bescherming van persoonsgegevens veel meer duidelijkheid geeft over wat je nu eigenlijk wilt doen. Je doet eigenlijk de bescherming van persoonsgegevens om de privacy van de betrokkenen te respecteren en daar goed mee om te gaan.

Beveiligingsmaatregelen
Er worden ook veiligheidsrondes gedaan waar F ook in meeloopt. F kijkt dan of er dingen zijn op het terrein van informatiebeveiliging of privacy die verbetering behoeven. Voorbeelden hiervan zijn papierkratten of computers die open staan, terwijl deze eigenlijk netjes vergrendeld moeten worden. Dit weet ook iedereen bij zorginstelling F, daar zijn gedragsregels over afgesproken.

Verschillende benaderingswijze voor verschillende groepen
Er wordt op dezelfde manier naar iedereen gecommuniceerd. F is van mening dat het niet uitmaakt wat je in de organisatie doet, voor iedereen gelden dezelfde regels. Daarom vindt F dat iedereen op dezelfde manier geïnformeerd moet worden over wat er van medewerkers verwacht wordt.

Maatregelen bij niet naleven regels
In zorginstelling F heerst een aanspreekcultuur. Dat betekent dat medewerkers opletten wat er gebeurt en elkaar erop aanspreken wanneer je dingen ziet waarvan je denkt dat dit anders hoort. Niet met het idee van dat je iets fout gedaan hebt, maar meer van joh denk er even aan. Er heerst hierbij een open sfeer.

Veranderingen in organisatie sinds invoering Meldplicht Datalekken
Mensen zijn wel een stuk alerter geworden. Je krijgt bijvoorbeeld vragen of er een betere manier is om documenten te versturen per mail. Zorginstelling F is nu aan het kijken naar een softwarematige oplossing om mails veilig te kunnen versturen.

Communicatie-inzet naar aanleiding van Meldplicht Datalekken
Zorginstelling F heeft een intranet, maakt gebruik van nieuwsbrieven en van postercampagnes. Daarnaast houdt F één keer per jaar een informatiebeveiligingsmarkt waarin ook privacy aan de orde komt. Dit jaar ging dit ook specifiek over de Meldplicht Datalekken. Deze markt houdt zorginstelling F voor de ingang van het restaurant, omdat daar veel medewerkers langslopen. Ze kondigen deze markt aan op intranet en kondigen het ook weer af op intranet door de highlights hierop te presenteren. Op deze manier worden ook mensen die die dag niet aanwezig waren op de hoogte gehouden. Maar daarnaast is het echt het belangrijkste om bij afdelingen langs te gaan en daar je verhaal te vertellen. Hier houdt F dan een verhaal over informatieveiligheid. F begint meestal met social media om aan te sluiten bij de werknemer en zijn privéleven en maakt vervolgens een bruggetje naar het werk. Centraal hierbij staat wat zorginstelling F van de medewerker verwacht po het gebied van informatieveiligheid.

Risico's van een datalek voor een instelling
Het belangrijkste is dat alle patiënten erop moeten kunnen vertrouwen dat hun gegevens bij zorginstelling F in goede handen zijn, dus dat willen ze uitstralen. Dit is lastig in een ziekenhuis, omdat iedereen naar binnen kan lopen. De Raad van Bestuur wordt daarnaast ook wakker als ze weten dat ze kans hebben op een boete van 820.000 euro.

Risico's in beeld bij bestuur
De Raad van Bestuur heeft de gevolgen goed in beeld. Los van die boete heb je als organisatie ook een klus die je moet uitvoeren als je met een datalek van doen hebt. Je moet ontdekken wat de oorzaak van het lek is, wat de gevolgen van het lek zijn en wat je daaraan kunt doen. Daarnaast heb je herstelwerkzaamheden als ziekenhuis om aan het basisprincipe te kunnen voldoen dat iedere patiënt op je moet kunnen vertrouwen.

Procedure Meldplicht Datalekken
Zodra je een datalek constateert is eigenlijk het eerste wat je moet doen zorgen dat F het weet. Medewerkers kunnen intern bij F melden. Dit weten zij onder andere door de presentaties van F. Daarnaast is het onderdeel van de procedure die vindbaar is op het kwaliteitsportaal. Toen zorginstelling F die procedure heeft

gepubliceerd, heeft de instelling dit ook in de lijn gecommuniceerd aan lijnverantwoordelijken die dat weer door kunnen zetten naar de rest van de lijn. Op deze manier is geprobeerd dit zo breed mogelijk op het netvlies te krijgen in de organisatie. Er zijn twee methodieken om een datalek te melden je kunt F mailen of bellen of iemand meldt een incident bij de helpdesk waarbij de melder nog niet doorheeft dat het om een datalek gaat. De helpdesk heeft de instructie om bij ieder incident na te gaan of dit een potentieel datalek is en kan dan een vinkje zetten als dit zo blijkt te zijn. Dan krijgt F dit via het systeem door. F is 24 uur per dag beschikbaar voor datalekken.

Meldingen
Er komen nog nauwelijks meldingen binnen. F heeft een tweetal datalekken gemeld. F denkt dat dit een goed teken is. F denkt dat zijn instructie helder is: 'als organisatie moet je je stinkende best doen om je medewerkers goed te informeren over wat een datalek is en hoe je dit moet constateren. Weet hier dat de drempel heel laag is en dat je bij iedere vorm van twijfel meteen moet bellen'. Het kan natuurlijk zijn dat medewerkers niet melden, maar F communiceert duidelijk dat F liever heeft dat een melding intern doorkomt dan dat een betrokkene, een patiënt of medewerker gaat melden bij de Autoriteit Persoonsgegevens.

Rol van de Autoriteit Persoonsgegevens
Het is goed dat ze er zijn, maar ze hebben te weinig mankracht en dat is wel echt een probleem. Er is nog geen boete uitgedeeld, terwijl dit wel noodzakelijk is als je als organisatie slagvaardig wilt kunnen optreden. De angst moet er wat F betreft meteen af: we moeten transparanter omgaan met dit soort incidenten om een hoger kwaliteitsniveau van de bescherming van persoonsgegevens te bereiken. Uiteindelijk moeten organisaties snappen dat de inzet is om zo goed mogelijk om te gaan met persoonsgegevens. Daarom verwijst F ook graag terug naar het basisuitgangspunt dat mensen erop moeten kunnen vertrouwen dat er goed omgegaan wordt met de gegevens van patiënten.
F geeft aan dat de AP een brief gestuurd heeft naar de Raden van Besturen van alle zorginstellingen, maar dat deze ging over autorisaties binnen het elektronisch patiëntendossier, verder horen ze van de Autoriteit niet zoveel. F heeft ze wel eens gebeld met een vraag. Die vraag is door de autoriteit nog niet beantwoord.

Voorbereiding op de AVG
Zorginstelling F is hier nog niet op voorbereid, maar is wel bezig zich hierop voor te bereiden. Voor deze organisatie heeft F in kaart gebracht wat de verschillen zijn tussen de WBP en de AVG en wat dit van de organisatie vraagt om de komende tijd op te pakken en uit te voeren. Daarbij moet je wel in je hoofd houden dat de AVG eigenlijk al is ingegaan, maar dat er pas vanaf mei 2018 op gehandhaafd wordt. Als je het heel netjes doet dan zou je dus op een zo kort mogelijke termijn ook compliant moeten zijn op de AVG. Nu is het niet zo dat er in de AVG heel veel nieuws staat .Als je je beleid als organisatie goed uitvoert dan zou je eigenlijk al voor 80% compliant kunnen zijn aan de AVG. Het gaat om die laatste 20%. Het is dan ook meer aanscherpen van wat we eigenlijk al aan het doen waren.
F heeft een actielijst opgesteld met wat er in de komende tijd uitgevoerd moet worden. De Privacy Impact Assessments gericht uitvoeren is bijvoorbeeld nog een stap die zorginstelling F nog goed in zijn proces moet inpakken.

Bekendheid 'ZEKER' campagne
F is bekend met de 'ZEKER' campagne van de NVZ, omdat die komt uit het netwerk informatiebeveiliging waar F ook lid van is. F doet zelf altijd in de weken van Alert Online de informatieveiligheidsmarkt en dan zie je ook de campagne 'ZEKER' voorbij komen. Hij haakt hier dan op in. Eén van de onderdelen van de informatieveiligheidsmarkt was bijvoorbeeld het invullen van de zekertest. Deze test kon je ter plekke invullen met een groot scherm zodat mensen konden meekijken.

6.7 Categorisatie interview zorginstelling G

Achtergrond van de Functionaris voor de Gegevensbescherming
G: 'Ik ben niet in dienst van deze zorginstelling, maar ik word ingehuurd. Juist ook voor dit specifieke onderwerp. Dus ja van ons uit heeft het zeker de aandacht en deze zorginstelling heeft het ook de aandacht gegeven die het nodig heeft en gevraagd of ik daar wat werkzaamheden voor wil verrichten als functionaris gegevensbescherming'.

G: 'Ik werk voor mezelf en vanuit die hoedanigheid ben ik hier terechtgekomen voor wat andere projecten nog en wat architectuurvraagstukken. Architectuurvraagstukken liggen redelijk dicht tegen het privacygedeelte aan en is in principe ook een onderdeel van de NEN 7510 architectuur. Dus in die hoedanigheid ben ik begonnen en met de nieuwe wetgeving en dergelijke is dat verder uitgebreid naar functionaris'.
Onderzoeker vraagt aan G of G voor meerdere zorginstellingen werkt G antwoordt: 'Ja'.
Onderzoeker vraagt hoeveel uur per week G ongeveer bij deze zorginstelling zit: 'Ja, ik zit hier een dag of drie per week gemiddeld'.
Onderzoeker vraagt of G voor de andere organisaties ook als FG werkt of ook wel eens in een andere functie G antwoordt: 'We zijn daar nu wel NEN 7510 aan het implementeren. Functionaris moet nog benoemd worden. We zijn net begonnen. Het zou maar zo kunnen dat ik dat ook word. Het zou ook kunnen dat ze intern iemand nemen'.
Onderzoeker vraagt hoe G bij deze instelling terecht is gekomen en of hij al andere werkzaamheden voor de instelling verrichtte G antwoordt: 'Ja, ik deed hier al andere werkzaamheden en ben dit erbij gaan doen zeg maar'.
Onderzoeker vraagt hoe lang G al voor deze instelling werkt G antwoordt: 'Ik loop hier denk ik zo'n drie jaar'.

Verhouding tussen privacy en de bescherming van persoonsgegevens
G: 'Ja, dat ligt heel dicht tegen elkaar aan wat mij betreft. Het één kan niet zonder het ander. Kijk de wetgeving is natuurlijk één, maar uiteindelijk is die ook weer gebaseerd op de NEN of de ISO-normen zeg maar en echt op privacy gericht'.

Belegging van de functie in de organisatie
Onderzoeker vraagt of G bij deze instelling dan de enige is die iets met privacy van doen heeft G antwoordt: 'Nou ja goed zo voelt het soms, maar dat is zeker niet de bedoeling. Informatiebeveiliging doe je niet alleen dat doe je als hele organisatie, maar het liefst stoppen ze het wel bij je weg en willen ze er het liefst zo min mogelijk mee te maken hebben. Maar goed als je het wilt borgen binnen de hele organisatie dan moet ook de hele organisatie ermee bekend zijn en je managementsysteem moet draaien, dat is het belangrijkste'.
G: 'Het zit bij een afdeling ja. Denk niet dat het daar hoort. ICT is onder andere één van zijn speerpunten zeg maar. Deze instelling is verdeeld in klantgroepen en een centraal deel, dus dit valt onder het centrale deel. Maar goed als je het goed bekijkt zou je rechtstreeks onder bestuurders en staffunctie moeten zitten denk ik. Nu heeft iemand er belang mee, maar in principe is dat niet de bedoeling'.
Onderzoeker vraagt of G wel bij iemand in de organisatie terecht kan als hij problemen heeft in bijvoorbeeld het beoordelen van een datalek G antwoordt: 'Ik kan wel bij mensen terecht ja even polsen hoe zij het zien en tot waar het gekomen is en wat er aan de hand is, maar goed ik ben daar wel altijd bij betrokken en ik doe altijd wel het advies dan of er wel of niet gemeld moet worden'.

Thema in beeld bij bestuur
Onderzoeker vraagt of het managementcommitment er nu nog niet is G antwoordt: 'Formeel nog niet nee. Ze weten zeker dat het de nodige aandacht heeft. Je hebt er continu discussie over, maar als je met de NEN en ISO bezig bent heb je echt managementcommitment nodig en het moet ook minimaal één keer in de maand op de agenda staan en vastgelegd worden wat daar besproken is en ook wat zijn de stukken die aangeleverd moeten worden. Dat moet volgend jaar echt ook gaan gebeuren zeg maar'.

Prioriteit van privacy in de organisatie
Onderzoeker vraagt of de vraag om ook FG te worden bij zorginstelling G van het bestuur kwam of… G antwoordt: 'We hebben, ja deels vanuit het bestuur, maar we hebben ook een risicoanalyse gedaan halverwege vorig jaar en daar kwamen deze punten naar boven zeg maar dus er is wel gevraagd vanuit de directie en vanuit het bestuur om dat op te pakken zeg maar. Niet zozeer om de certificering te gaan halen, maar wel om volgens die weg te gaan werken. En ook om te zorgen dat de transformatie die ze nu doormaken om alles uit te besteden dat leveranciers wel gelijk aan de dingen voldoen waar ze aan moeten voldoen volgens ons'.
G: 'Het krijgt de juiste prioriteit ja. Ze zijn er zeker van bewust dat het impact heeft'.
Onderzoeker vraagt aan G waaraan je dat dan bijvoorbeeld kunt zien G antwoordt: 'Er wordt snel gereageerd op mail of er wordt van hun kant uit: je wilt natuurlijk dat je alles hoort en ziet, maar dat gaat natuurlijk niet zo, dus ook vanuit die weg zijn er kanalen natuurlijk en worden er dingen besproken met andere directeuren van

wat er eventueel gebeurd is en dan word ik wel meteen in de loep gezet zeg maar om te kijken hoe we dat kunnen afdekken en of er echt nog iets gemeld moet worden zeg maar'.

Wie stelt beleid op
Antwoord van G op vraag van onderzoeker of G dingen schrijft voor beleid: 'Negen van de tien keer schrijf ik het en als een ander het schrijft dan kijk ik of dat het past in het totaalplaatje, ja'.
Antwoord van G op vraag of G daarvoor met Raad van Bestuur overlegt: 'Ja, ik overleg altijd en ik adviseer altijd als ik het zelf geschreven heb om dat te accorderen zeg maar en als een ander dat geschreven heeft wat ik ervan vind en ook om het te accorderen. Ja, de Raad van Bestuur is daar altijd bij betrokken, die is ook hoofdelijk aansprakelijk'.

Samenwerking met communicatieafdeling
G: 'Ja, een stukje awareness en dat soort zaken doen we altijd gezamenlijk'.

Informatie over de instelling
Onderzoeker vraagt of deze instelling meerdere locaties heeft G antwoordt: 'Ja, dit is echt alleen een kantoor zeg maar en er zijn nog 12 grote locaties waar zorg verleend wordt en dan nog een stuk of 12-13 locaties met wijkteams. De teams die echt de wijk in gaan zeg maar voor de extramurale zorg'.
Onderzoeker vraagt hoeveel verschillende managers er zijn G antwoordt: G: 'Nou we hebben twee bestuurders en er zitten vier klantgroepen dus vijf directeuren daar zitten, die wekelijks overleg houden, dus daar moet het vandaan komen dan zeg maar'.

Communicatie-inzet informatiebeveiligingsbeleid
G: 'We hebben laatst geflyerd met een aantal speerpunten en ook materiaal rondgemaild. Nieuwsbrieven doen we en we zorgen dat het dan op alle locaties ligt op plekken waar mensen komen. Aan de wand gespijkerd ja'.
G: 'We hebben ook een awarenesstraining die verplicht is om te doen door iedereen'.
Onderzoeker vraagt of de training verplicht is voor nieuwe medewerkers en of huidige medewerkers hem ook hebben gedaan: 'Ja en de huidige medewerkers die moeten hem voor het eind van het jaar gedaan hebben'.
Onderzoeker vraagt wanneer deze training is opgezet, G antwoordt: 'Even kijken hoor dat is in ja, we hebben hem al een tijdje zal ik maar zeggen. Maar door de veranderingen en het kantelen van de organisatie hebben we iedere keer een excuus gehad om hem niet te gaan doen zeg maar. En nou ja er is nu wel gezegd in volgens mij september ofzo is die beschikbaar en tot het eind van het jaar hebben de mensen om hem gewoon te gaan doen'.
Onderzoeker vraagt wat er dan bijvoorbeeld in die training staat G antwoordt: 'Ja, het is een online training voor awareness, voor informatiebeveiliging. Dus het zijn iets van 20 punten geloof ik waar je gevraagd wordt wat wel of niet goed is en als je antwoord hebt gegeven dan staat erachter een verklaring van waarom dat zo is met wat verdere tekst en uitleg'.
Onderzoeker vraagt of het een soort multiplechoicevragen zijn met uitleg erbij G antwoordt: 'Ja, met uitleg erbij waarom iets goed of fout is of wat de beargumentering is in ieder geval'.
Onderzoeker vraagt hoe lang het ongeveer duurt om het in te vullen G antwoordt: 'Uh, ze zeggen twintig minuten, maar je bent wel wat langer bezig'.
G: 'Een half uur tot drie kwartier ben je wel zoet als je dat gewoon doet. Ook als je het goed hebt alsnog alles gaat doorlezen wat er dan achter staat'.
Onderzoeker vraagt of er op dit moment al geïnformeerd wordt aan medewerkers dat ze dossiers niet mee mogen sturen via de mail G antwoordt: 'Ja, ja zeker. Ze weten ook dat het niet mag. Ik zeg niet dat het niet meer gebeurt, maar als het naar boven komt dat het gebeurt dan wordt er ook echt wel actie ondernomen en dan wordt er naar de afdelingen toegegaan om het te bespreken, maar goed zeggen dat iets niet mag vind ik altijd wel heel makkelijk. Je moet ook een alternatief aanbieden en daar zijn we mee bezig'.
Onderzoeker geeft aan dat dat ook lastig is als er geen alternatief is dat je dat ook bij Google ziet G antwoordt: G: 'Nou ja bij Office 356 heb je bijvoorbeeld One Drive daar kun je eigenlijk hetzelfde mee als met Dropbox, je hebt Jemmer erin zitten. Dat is voor jouw organisatie net allemaal iets betrouwbaarder dan dat je dat bij de gratis versies doet. Er is niks gratis hè. Het is in ieder geval de informatie die jij aanlevert waarvoor jij betaalt en daar gebeurt van alles mee, dus daar moet je alternatieven voor verzinnen. Hoe wil je dat zoveel mogelijk afdichten, ook in je keten. Als je voorop loopt dan moet de rest ook nog mee hè'.

Verschillende benaderingswijze voor verschillende groepen
G: 'Daar wordt wel onderscheid in gemaakt tussen extramuraal en intramuraal ja. Dat zit anders in elkaar extramuraal loopt iedereen met Ipads of met dossiers op de fiets. Die komen echt bij de mensen thuis dus daar spelen wat andere dingen dan bij de teams die binnen zitten, wat in principe afgesloten ruimtes zijn. Ja dan werkt het iets anders'.
Onderzoeker vraagt aan G hoe je de mensen bereikt die altijd onderweg zijn G antwoordt: 'Ja, eigenlijk op dezelfde manier. Daar wordt ook geflyerd en wordt ook gesproken. We hebben ook een awarenesstraining die verplicht is om te doen door iedereen'.

Bekendheid 'ZEKER' campagne
G: 'Dat is de flyercampagne die we gedaan hebben'.
G: 'Ja, klopt. Twee weken ofzo was dat hè. Dus toen hebben we iedere keer wat gecommuniceerd en neergelegd'.
Onderzoeker vraagt of ze dan ook die online test gebruikt hebben, G antwoordt: 'Ik heb hem zelf wel gedaan, maar we hebben hem niet gebruikt. Omdat we ook zelf al een test of een training hebben lopen, vond ik het een beetje dubbel. Dus dat hebben we niet gedaan. Maar dat is misschien voor een vervolg weer wel een goede optie'.
Onderzoeker vraagt wat G van die test vond G antwoordt: 'Ik zit even te denken, ik heb hem toen gedaan, maar ik zou het zo niet meer weten wat ik ervan vond'.
G: 'Ja, het kwam een beetje overéén zeg maar en het is voor kantoormedewerkers wat we hebben en met mail maar ook gewoon fysiek. Mag je een foto maken van iemand om te kijken met je collega hoe je daarmee om moet gaan of zoiets. Nou dat mag van iets, maar niet herkenbaar en dat soort dingen. Whatsapp hè mag je dat gebruiken en dat soort dingen allemaal. Dus echt heel breed zeg maar opgezet en dat is op zich wel goed'.

Inrichting informatiebeveiligingsbeleid
G: 'Er zijn sowieso gedragsregels. Niet specifiek voor informatiebeveiliging op dit moment. Er is wel een soort van protocol waarin de standaardzaken staan, maar dat is echt niet veel bijzonders. Dat is dat je elkaar moet aanspreken op een aantal zaken, usb en dat soort dingetjes, clean desk, nou dat zijn een beetje de standaard punten'.

Risico's voor instelling van een datalek
G: 'Van een datalek? Ja, dat ligt eraan op welk gebied het lek is zal ik maar zeggen of het een cliëntdossier is of alle cliëntdossiers dan haal je het acht uur journaal wel, we zijn natuurlijk een redelijk grote club. Dus ja dan heb je wel een probleem'.
Onderzoeker vraagt aan G op welk gebied je dan een probleem hebt, G antwoordt: 'Nou in ieder geval dat alles op straat ligt en dat je de verkeerde aandacht krijgt als organisatie zijnde. Dus op dat gebied zeker en je krijgt een boel werk. Je moet al je cliënten af je moet ze allemaal informeren en allemaal voortgang doen en ja dan wordt er nog een keer bovenop je huid gezeten om maatregelen te nemen en dan is het eigen tempo wel weg zal ik maar zeggen'.

Risico's in beeld bij bestuur
G: 'Nou ja goed zijn deze gevolgen in beeld bij het bestuur, ja dat ligt eraan of je een boete gaat krijgen of niet. Alle punten die er zijn gaan sowieso altijd via het bestuur. De bestuurders zijn altijd op de hoogte van de incidentmeldingen'.

Veranderingen in organisatie sinds Meldplicht Datalekken
G: 'Ja, je merkt wel dat het wat meer aandacht heeft ook vanuit het management zeg maar het is iets minder vrijblijvend geworden. Het speelt natuurlijk al langer, dat je er iets mee moet en dat het aandacht nodig heeft. Maar met de nieuwe wetgeving en ook de consequenties daarvan is het wel allemaal ietsjes makkelijker geworden om acties te ondernemen zeg maar'.
Onderzoeker vraagt of je dan ook verschil merkt dat je makkelijker beleid kan opstellen G antwoordt: 'Je merkt dat het nu wat makkelijker gaat. Dat is niet helemaal eerlijk misschien want we zitten midden in een omslag om alles uit te gaan besteden dus dan moet je sowieso alles op papier gaan zetten en zorgen dat het er is. Om sowieso een referentiekader te hebben en je eigen uitgangspunten helder te hebben, dus het is niet helemaal één op één dat dat door de wetgeving komt, maar dat werkt wel mee zeg maar'.

Onderzoeker vraagt in wat voor overgangsfase G zit of dat is dat er meer uitbesteed gaat worden G antwoordt: 'Ja, applicaties die buiten de deur komen te staan'.
Onderzoeker geeft aan dat daar waarschijnlijk ook veel bewerkersovereenkomsten aan vast liggen G antwoordt: 'Ja, dat is wel leuk ook om dat voor elkaar te krijgen'.
G: 'Nee, dat is een hele lastige. Iedereen moet in principe een bewerkersovereenkomst hebben als je diensten verleend voor een ander, maar er zijn ook bedrijven waarvan ik denk ja hoezo dat wil ik helemaal niet. Ja mooi dat jij dat niet wilt maar je bent verplicht om dat te hebben en dat is niet sinds 1 januari dat is al anderhalf jaar zo. Dus het had er eigenlijk allang moeten zijn en dan nog over de inhoud zeg maar. Dus we hebben het zelf opgesteld eentje en ja je hebt altijd discussies over wat wel kan en wat niet kan, dus het is wel altijd een dingetje zeg maar'.

Communicatie-inzet naar aanleiding van Meldplicht Datalekken
Onderzoeker vraagt aan G of er bijvoorbeeld geïnformeerd is aan medewerkers dat de wet er is G antwoordt: 'G: Ja, ja zeker dat is allemaal gecommuniceerd ja'.
Onderzoeker vraagt op wat voor manier dat dan is gegaan G antwoordt: 'Dat is via de directeuren gegaan dat dat naar hun afdeling en mensen bekend is en daar hebben we, dat is onderdeel van de awareness, daar flyeren we ook voor en daar sturen we mailtjes voor, de nieuwsbrief en op de intranetpagina staan daar regelmatig stukken over van ja waar je je aan moet houden'.
Onderzoeker constateert dat het dus eigenlijk onderdeel is van de awarenesscampagne die er is G antwoordt: 'Ja, ik zie het niet los zeg maar. We zijn dan met de NEN 7510 bezig om in ieder geval die werkwijze te hanteren en daar is dit onderdeel van. Omdat ministeries ook aangeven dat als je de NEN 7510 hanteert dat dat in principe voldoende moet zijn. Ze zijn daar voorzichtig in natuurlijk, dat snap ik ook, maar ja dat dat wel de weg is, dus ja dan hoef je daar niet nog een keer naast nog iets te doen'.
Onderzoeker vraagt of G dan op zo'n afdeling presentaties gaat geven of iets dergelijks (na dit antwoord van G op de vraag van onderzoeker of er maatregelen zijn als mensen bijvoorbeeld hun computer open laten staan: 'Je moet elkaar daarop aanspreken. Dat zijn dingen dat kost best wat tijd zeg maar. Daarom vind ik ook dat ik dat niet alleen moet doen maar dat het ook breed gedragen moet worden. En daar zijn we nu ook mee bezig dat het vanuit het managementsysteem wat moet gaan lopen zeg maar. Een afdeling als kwaliteit mee te nemen in dit verhaal want die kijken echt naar medische stukken en naar cliëntveiligheid en dat soort zaken, maar hè dit is een kleine stap om erbij te doen denk ik dan'). G antwoordt: 'Ja, dat doe ik middels presentaties, maar ook gewoon het onderdeel maken van het werkproces dat ze daar ook een actieve rol in hebben. Dus niet alleen informatief maar ook dat zij een onderdeel zijn van het geheel en zorgen dat ook daar gemeld kan worden en dat ook zij acties uit gaan zetten'.

Procedure Meldplicht Datalekken
G: 'Ze weten waar en hoe ze moeten melden en dat is ook gepubliceerd en regelmatig gecommuniceerd'.
G: 'Ja, nou er is een intern meldpunt maar dat komt ook wel bij mij uit. Dus ja dat is er zeker. We hebben één keer in de maand ook een inloopspreekuur voor als mensen vragen hebben en daar wordt op zich ook wel gebruik van gemaakt dat mensen binnenlopen of telefonisch dat mensen echt wel komen van wij doen dat altijd op deze manier maar dat voelt niet goed'.
Onderzoeker vraagt of iedereen in principe langs kan komen op het spreekuur G antwoordt: 'G: Ja, vanuit de hele organisatie ja'.
G: 'In principe hier en dat kan ook op een locatie als dat nodig is ja'.
Onderzoeker vraagt of er veel animo is voor dat spreekuur G antwoordt: 'Ja, wat is veel?'
Onderzoeker vraagt of er mensen langskomen G antwoordt: 'Er is denk ik vier keer wel via de mail of via de telefoon gevraagd hoe moet ik dit nu zien en hoe moeten we hier nu mee omgaan?'
Onderzoeker vraagt of er alleen bij G gemeld kan worden of dat het ook in het kwaliteitssysteem zit verwerkt G antwoordt: 'Nee, dat zit nog niet in het systeem verwerkt. Daar zijn we nu wel mee bezig'.
Onderzoeker vraagt of G meer begonnen is met het meekrijgen van de medewerkers of met… G antwoordt: 'Nou met de medewerkers meekrijgen sowieso en zorgen dat er technisch een aantal dingen georganiseerd en gedaan zijn en ja we moeten er nu echt naar toe zeg maar om ook het managementcommitment te hebben'.
Onderzoeker vraagt of die in de Raad van Bestuur zitten G antwoordt: 'Ja, die zitten ook in het managementgeheel zeg maar'.

Bijdrage van communicatie om risico's in te perken

G: 'Nou Awareness is communicatie denk ik, dus dat is 80% van het hele gebeuren is awareness en communicatie dus ik denk dat een heel groot deel daarvan de boel kan afdekken'.

Voorbereiding op de AVG
G: 'Nou dat is hetgeen waar we naartoe werken. Dan gaat het echt pijn doen vanaf dat moment als je het niet op orde hebt. Er verandert wel wat natuurlijk'.
Onderzoeker vraagt hoe G van plan is daarop voorbereid te gaan zijn G antwoordt: 'Door te zorgen dat je op de NEN-manier werkt dat je dat geadopteerd hebt en dat je volgens die weg werkt dat je je managementsysteem op orde hebt zeg maar. Kijk dat er nooit iets gebeurt dat kan je toch niet afdekken, dus je moet gewoon zorgen dat je managementsysteem loopt en zorgen dat je in control bent. Dan kun je ook schakelen als er iets gebeurt'.
Onderzoeker vraagt wat dan concrete voorbeelden zijn die doorgevoerd moeten zijn in de organisatie G antwoordt: 'Nou het zijn iets van 135-140 controls die je als organisatie moet beantwoorden hoe je daarmee omgaat. Dus die moet je één voor één af en dan aan de hand van de business impact en de risicoanalyse kan je ze kwalificeren en dan kan je zeggen degenen die de meeste pijn doen alvast behandelen en zorgen dat je dat op orde hebt. Als je naar de NEN kijkt heb je drie jaar de tijd om alles te doen en ja dat moet je dan herhalen verbeteren en zorgen dat dat in control is. Dus dat is het idee aan de norm. Maar die is gelijk aan de ISO70001'.
Onderzoeker vraagt of dat de norm is waar je eigenlijk nu al aan moet voldoen G antwoordt: 'De zorginstelling hoeft daar niet aan te voldoen. Ziekenhuizen die zijn het wel verplicht en die hebben vijf jaar de tijd gehad en iedere keer een stapje verder. Dat is bij de VVT-markt in ieder geval nog niet zo geïntroduceerd en je bent het ook niet verplicht, maar ja hoe lang duurt het voordat het wel verplicht wordt en als het verplicht wordt dan krijgen ze niet de vijf jaar die het ziekenhuis ook heeft gehad zeg maar. Dus daarop zijn we ook al wat aan het voorsorteren en sowieso mei 2018 moet je het denk ik op orde hebben. Dat lijkt me verstandig'.

Rol van de Autoriteit Persoonsgegevens
G: 'Ja, geen idee. Ja, ik vind hem lastig. De wetgeving is er en ze zijn redelijk rustig zal ik maar zeggen, maar ik vrees wel dat ze nog voor mei 2018 een paar eruit vissen die als voorbeeld gesteld gaan worden en daar kan je beter niet bij zitten zeg maar'.
Onderzoeker vraagt of G informatie heeft ontvangen toen de wet inging van de AP G antwoordt: G: 'Nee, volgens mij helemaal niks. We hebben onszelf aangemeld als functionaris, we staan al op de site en dan krijg je een paar mailtjes van hoe het werkt en hoe je je aanmeldt. Maar voor de rest volgens mij is er niks van hun kant uitgekomen van dat het er is'.
Onderzoeker vraagt of G zelf al eens contact opgenomen heeft met de AP G antwoordt: 'Ik heb ze één keer gebeld volgens mij om te kijken om iets wel of niet aan te melden. Daar kreeg ik niet echt een goed antwoord op zeg maar. Dus dat heb ik zelf bekeken aan de hand van de vragen die ze hebben als je moet melden, maar uiteindelijk hebben we twee of drie keer op het punt gestaan om iets te melden, maar uiteindelijk niet gedaan omdat je gewoon wel kon borgen dat er niks gelekt was en dat er eigenlijk niks naar buiten is gekomen'.
Onderzoeker vraagt of G geen antwoord of reactie van hen heeft gehad G antwoordt: 'Nou niet iets waar ik mee verder kan'.

Maatregelen bij niet naleven regels
Onderzoeker vraagt of er op dit moment al maatregelen zijn voor medewerkers als ze dingen niet melden G antwoordt: 'Nee'.
Onderzoeker vraagt als ze bijvoorbeeld hun computer open laten staan G antwoordt: 'Je moet elkaar daarop aanspreken. Dat zijn dingen dat kost best wat tijd zeg maar. Daarom vind ik ook dat ik dat niet alleen moet doen maar dat het ook breed gedragen moet worden. En daar zijn we nu ook mee bezig dat het vanuit het managementsysteem wat moet gaan lopen zeg maar. Een afdeling als kwaliteit mee te nemen in dit verhaal want die kijken echt naar medische stukken en naar cliëntveiligheid en dat soort zaken, maar hè dit is een kleine stap om erbij te doen denk ik dan'.
Onderzoeker vraagt of er ook veiligheidsregels zijn zoals bijvoorbeeld het gebruik van usb-sticks G antwoordt: 'Daar zijn beperkte regels voor. In ieder geval dat je erop moet letten en sticks die niet van jezelf zijn niet gebruiken, maar dat is redelijk beperkt. En we zijn ook aan het kijken of het sowieso nog nodig is om de usb open te laten staan, zodat het helemaal niet meer kan gebeuren'.
Onderzoeker vraagt of G dan nu samen met de afdeling kwaliteit aan het kijken is hoe dit soort dingen aangepakt moeten worden G antwoordt: 'Ja, hoe we dit gaan borgen'.

Onderzoeker vraagt of de implementatie daarvan nog een beetje moet komen G antwoordt: 'Ja dat zal begin volgend jaar volgen'.

Evaluatie van beleid
G: 'Ja, er komen sowieso vragen over van waarom iets is zoals dat aangegeven is of dat het eigenlijk veels te makkelijk is. Dan denk ik heel goed ik hoop dat dat voor iedereen geldt, want ja zo makkelijk is het dan toch ook weer niet. Maar we proberen daar wel van te leren zeg maar en je krijgt daar wel discussies over en dat is onderling, maar ook naar het management toe dat er dingen anders moeten of iets dan wel moet ja bijvoorbeeld al met Whatsapp. Het is makkelijk te vinden en bereiken voor thuis gebruik je het ook dus je weet allemaal hoe het werkt. Het is alleen jammer dat het van Facebook is en dergelijke en die kunnen er alles mee doen wat ze willen. Dus je moet het gewoon niet gebruiken en hetzelfde geldt voor mail, daar kan je ook geen dossiers mee versturen of informatie dat soort dingen mag ook niet'.

Lastige punten om groepen te bereiken
G: 'Nou ja goed als je in een keten zit, dus het gaat van ziekenhuis naar zorginstelling naar de apotheek en die gegevens moeten wel rond zeg maar dus hoe doe je dat? Mail is dan best makkelijk zeg maar en vroeger werd er gefaxt, faxen gebeurt nog steeds, maar ook dat kan niet meer hè in ieder geval niet in de zin van bij de receptioniste waar alles binnen komt. Dat moet weer via een beveiligde printer, dus dat is allemaal wat strikter geworden. Maar ja als een huisarts zegt, ja leuk al die onzin maar ik doe er niet aan mee dan is dat wel de zwakste schakel zal ik maar zeggen. En ja die zijn er nog steeds, die het niet zo belangrijk vinden. Die gmail gebruiken bij wijze van spreken Dus ze zijn er allemaal nog'.
G: 'Ja er zijn best veel leveranciers waar de dossiers in zitten en hoe ga je dat onderling communiceren?'
Onderzoeker geeft aan dat dat ook een lastige is G antwoordt: 'Ja, dat krijg je er allemaal gratis bij'.

6.8 Categorisatie interview zorginstelling H

De functie van Functionaris voor de Gegevensbescherming
H1: 'Ik ben hier terechtgekomen via de zorgadministratie. Dat is eigenlijk alle gegevensbewerking rondom de patiënt en vanaf eind jaren 80 heb ik ook al in de commissie privacybescherming gezeten en dat heeft ook altijd mijn warme belangstelling gehad. En ik ben tot drie jaar geleden manager geweest van de afdeling zorgadministratie. En dit is iets wat ik heel graag in mijn laatste fase in mijn carrière zou willen doen, echt weer de inhoud in, dus zo ben ik hier terechtgekomen. En het voordeel van mijn achtergrond is dat ik eigenlijk toch wel vrij veel weet van de gegevensverwerkingen van deze organisatie en ook daarbuiten. Ik dacht dat ik redelijk wat wist over de wetgeving. Nou daar zit ik nu voor in een scholingsprogramma om dat helemaal ook goed in de vingers te krijgen. Het duurt drie jaar in totaal en je hebt gemiddeld elke zes weken een tentamen of een workshop. Je moet studiemateriaal bestuderen en dan krijg je een workshop en een tentamen en ik leer daar waanzinnig veel'.
Onderzoeker geeft aan dat de opleidingen wel erg verschillen: sommige cursussen duren bijvoorbeeld 10 dagen en dan krijg je al een certificaat H1 antwoordt: 'Ik ben er ook van overtuigd nu al dat het gemiddelde niveau van een functionaris gegevensbescherming te laag is. Domweg ook omdat het beroep eigenlijk niet gedefinieerd is en in de wet staat gewoon dat diegene voldoende kennis en vaardigheden moet hebben om die functie uit te voeren, maar daar komen we niet mee weg als je kijkt naar met wat voor vraagstukken wij te maken hebben en de kwetsbaarheid van de organisatie en de afwegingen die gedaan moeten worden dan is het toch wel van belang dat diegene redelijk geschoold is. Niet alleen in het wettelijke gedeelte, maar anderzijds moet je ook de afwegingen kunnen maken dus het ethische deel zal ik maar even zeggen. En dat betekent in feite dat je een afweging kunt maken tussen alle verschillende belangen die er zijn en dat je tot een afgewogen advies kunt komen. Dus dat is een subtiel spel'.
H2: 'Ik ben hier 13 jaar geleden binnengekomen als kwaliteitsfunctionaris bij één van de onderzoeksinstituten en daar kwam ik erachter van 'hee wij moeten al onze onderzoeksprojecten bij het College Bescherming Persoonsgegevens melden'. Dat is niet heel erg handig, maar je kan ook melden bij de functionaris gegevensbescherming van de organisatie en sindsdien ben ik FG voor het onderzoeksinstituut en sinds een jaar of drie vier ben ik dus functionaris gegevensbescherming van al het onderzoek en onderwijs heb ik er ook bij gekregen'.
H1: 'Onderzoek en onderwijs heel eigen karakter, heeft eigen risico's. En ik doe dan zorg en de s-voering'.

Belegging van de functie in de organisatie

Onderzoeker vraagt of er naast H1 & H2 nog andere FG's zijn in de organisatie H1 antwoordt: 'In feite niet formeel aangemeld maar we vormen in totaal een team van vier personen. Dat zijn drie FG's bij elkaar die dat niveau en de kennis hebben en één iemand die moet ons een beetje bij de les houden en die is de documentalist'.
Onderzoeker vraagt hoe dit team onderverdeeld is in de organisatie H1 antwoordt: 'Wij vormen een team. H2 zit in de divisie waar onderzoek plaatsvindt en ik zit bij bestuurlijke en juridische zaken, dus dat is het bureau van de Raad van Bestuur, maar ik heb daar natuurlijk een onafhankelijke positie in. Ik ben toezichthouder, want het zijn wettelijke taken voor ons tweeën. De belangrijkste zijn denk ik: toezichthouden, adviseren en awareness. Dat zijn onze kerntaken'.
H2: 'Onze afdeling heet eigenlijk privacybescherming en informatiebeveiliging. Dat loopt enorm in elkaar over'. We werken dus ook in een netwerk met mensen die zich daarmee bezighouden, dus informatiebeveiliging wat veel technische kanten heeft, samen met de technical security officer van de ICT-afdeling, maar ook met hoofd veiligheid als het gaat om fysieke gegevens en dergelijke'.
H1: 'Eigenlijk is het netwerk nog groter, want wij werken met z'n vieren samen maar we werken ook met de bedrijfsjuristen samen, met de gezondheidszorgjuristen werken we samen, Hoofd Veiligheid en met de technical security officers van de ICT-afdeling, daar vormen we eigenlijk een eenheid mee'.
H2: 'Heel breed, maar de problematiek is ook breed'.

Verhouding tussen privacy en de bescherming van persoonsgegevens
H1: 'Nou wij zien privacybescherming dat is eigenlijk de hele Wet Bescherming Persoonsgegevens en alles wat daarbij hoort'.
H1: 'Maar wij zeggen dat heeft met elkaar te maken, want informatiebeveiliging dat is eigenlijk in feite de uitwerking van artikel 13 dat je technische en organisatorische maatregelen neemt. En voor ons is voor de informatiebeveiliging de NEN7510 norm en die willen we dan geïmplementeerd hebben en daar willen we als gecertificeerd zijn.

Wie stelt beleid op
H1: Wij zijn wel de trekkers, maar wij mobiliseren onder andere natuurlijk dat hele netwerk en de rest van de organisatie en we zorgen ook dat we de opdracht hebben in feite ook van de Raad van Bestuur, maar wat eruit komt, dus het informatiebeveiligingsbeleid daar staat natuurlijk de Raad van Bestuur vierkant achter en wij doen alleen maar mensen bij elkaar brengen en zorgen dat het op papier komt.

Thema in beeld bij bestuur
Onderzoeker vraagt of ze wel met het thema bezig zijn H1 antwoordt: 'Ja, volledig'. H2 antwoordt: 'Zij zijn daar niet zo blij mee, maar dan heb je het over de datalekken'.
H1: 'Klein stukje historie. We hebben bij deze instelling een aantal jaren terug een incident gehad, waarbij onze instelling op een behoorlijke manier de privacy geschonden had van patiënten. Dat is een rel geworden van jewelste. Maar als je dat even doortrekt naar de Raad van Bestuur, die dat ook opgevallen is en daarmee door dat incident is privacybescherming bij deze instelling hoog op de prioriteitenlijst gezet. Daarom zijn wij er ook daarom zijn wij ook benoemd en geregistreerd en weet ik het allemaal. De Raad van Bestuur heeft dit als vast onderwerp en een van de leden van de Raad van Bestuur heeft dit ook in zijn portefeuille en daar hebben wij ook regulier overleg mee en wij moeten ook op regelmatige basis rapporteren aan de Raad van Bestuur hoe de zaken ervoor staan. Daarbovenop worden we twee keer per jaar door externe audits ge-audit'.
H2: 'Maar dat gaat meer over de informatiebeveiliging'.

Samenwerking met communicatieafdeling
H1: 'Die heeft een prachtige site gemaakt voor de privacybescherming en informatiebeveiliging. Met name ook over social media waar in dit geval nogal wat risico's aan verbonden zijn. Alle uitingen die gemaakt worden in het kader van awareness, rondom privacybescherming of informatiebeveiliging lopen via een vast contactpersoon op de afdeling communicatie die zit ook in de commissie privacybescherming en informatiebeveiliging'.

Bekendheid 'ZEKER' campagne

H1: 'Daar hebben we ook aan meegedaan gedeeltelijk. Er zijn een aantal berichten via onze reguliere media het huis in gegaan om de privacybescherming te bevorderen op basis van die campagne. We hebben niet volledig met die campagne meegedaan. Ik weet niet meer precies wat wel en wat niet'.
H2: 'Nou ja de voorbeelden die ze hadden van bijvoorbeeld met zo'n middag zetten ze een boef erin tussen de wachtkamer. Dat vond ik niet zo aansprekend'.
H1: 'Nee, het was niet zo aansprekend. We hebben wel meegedaan, alleen we hebben er wat eigen ideeën aan gegeven'.
H1: 'Nee, je bent dom als je niet meedraait, want er wordt ook wel gewoon landelijk aandacht aan besteed en als je dan niets doet in je eigen huis, dat is niet best. Maar die campagne werd door ons niet als heel erg adequaat bestempeld'.
H1: 'Wel aandacht aan besteed in die periode via die artikelen en dergelijke maar niet specifiek die test'.

Awareness vergroten
Onderzoeker vraagt wat H bijvoorbeeld doet aan awareness H2 antwoordt: 'Dat hangt er ook een beetje vanaf over welk terrein je het hebt. Wij zijn een redelijk uitzonderlijk UMC, dat ik er namelijk ben. Zoveel aandacht voor research is er niet. En voor een deel is het allemaal in het research ingebakken. Een heleboel van ons onderzoek gaat langs de medische ethische toetsingscommissie, ken je die?'
H2: 'En deze toetsingscommissie kijkt is iets WMO(Wet Maatschappelijke Ondersteuning) of is iets niet WMO. Als het WMO is dan gaat het door een heel circus heen en niet WMO dan is het bij de meeste UMC's ga je gang maar. Hier kijken wij dan erg sterk naar de privacy. En daarin creëer je ook een stuk awareness. Bijvoorbeeld het woord anoniem ben ik aan het uitbannen. Dan staat er: uw gegevens zullen anoniem zijn. Nee, wij weten wie die persoon is dus dat kun je niet zo opschrijven. En dat is ook een stukje opvoeden van de organisatie wat daar ook in zit, dat zit er eigenlijk structureel in'.
H1: 'Nou wat we op dit moment doen: we hebben sowieso van die posters, do's en don'ts die zie je nog steeds hangen, we doen gebouwrondes. Iedere twee maanden doen we zo'n gebouwdeel en dan leggen we een soort kaarten neer met smileys met achterop wat wel en niet kan. Of afkeurend met andere woorden dit is niet in orde wat ik hier tegenkom. We merken dat dat een heel sterk awareness bevorderend effect heeft, want als we ergens een ronde gedaan hebben, worden we meteen heel vaak gebeld van waarom dat zo is. En daarnaast zie je die kaarten her en der. We hebben op de site, we hebben een eigen site of eigenlijk twee één voor privacy en informatiebeveiliging, maar ook voor bewust met social media omgaan. Dat is voor ons namelijk ook een bedreiging van de privacy van medewerkers en van de patiënten kan dat zijn. We hebben als mensen binnenkomen dan worden ze via een obligaat praatje of in ieder geval is dat geautomatiseerd worden ze meegenomen wat privacybescherming, informatiebeveiliging en beroepsgeheim betekent' (dit is intern voor nieuwe medewerkers).
H1: 'Nou daarnaast wat we ook wel doen aan awareness, hebben we regelmatig als er een issue is correspondentie met afdelingen. Als er iets belangrijks is zoals een datalek of ik noem maar wat dan komt dat ook in ons weekblad. Als er ernstige incidenten zijn bijvoorbeeld dat betekent ook dat we er aandacht aan besteden van 'héé we zien dit ook vaak terugkomen dus dan komt er weer een artikeltje om de awareness te bevorderen'. Alles bij elkaar genomen onder de streep vinden we het volstrekt onvoldoende, want hier in de organisatie wordt gebrek aan awareness als een heel groot risico gezien dat merken wij ook als wij die incidenten afhandelen: hoe halen ze het in hun hoofd om dit gedaan te hebben weet je wel. En dat komt toch omdat mensen nou het begint bij awareness als je je bewust bent van iets dan ga je daarnaar handelen dus dat is fase 1. Nou volgens mij hebben ze die fase 1 nooit doorlopen. En we willen nu ook dat gaan we nu ontwikkelen, e-learningmodules op het gebied van privacybescherming en informatiebeveiliging die verplicht worden voor alle medewerkers maar wel wat meer toegesneden op de groepen, want informatiebeveiliging en privacybescherming betekent iets anders voor mensen in de zorg zoals dokters of verpleegkundigen, maar het betekent ook weer wat anders voor mensen die bij ondersteunende afdelingen werken of voor onderzoekers. Dus op die manier, als je dat niet doet dan worden je bevoegdheden ingetrokken, zo willen we eigenlijk de awareness erin stampen'.
We hebben ook in het kader van de awareness een zogenaamde contactpersonenbijeenkomst. Eigenlijk in feite heeft iedere afdeling, als ze allemaal zouden komen zou het heel mooi zijn, een contactpersoon privacybescherming en informatiebeveiliging. Daarvoor organiseren we kwartaalbijeenkomsten om allerlei onderwerpen te bespreken. Dat zijn eigenlijk onze ambassadeurs op de afdelingen. Nou je voelt al wel aan dat wordt op verschillende manieren ingevuld. De één is heel actief en de ander die gaat erheen die gaapt drie keer eet zijn broodje op en gaat weer terug'.

H2: 'Ja, dat hangt ook van de aanpak af. Waar ik wat meer heen wil is dat we ze een soort pakketjes aanbieden. Bijvoorbeeld een powerpoint met een vraagstelling erop, twee sheets die in je werkoverleg gebruikt kunnen worden om op de afdeling te bespreken'.
Onderzoeker vraagt of het dan wat vaker terugkomt maar misschien in lichtere vorm H2 antwoordt: 'Lichtere vorm en praktisch'.
Wat ook belangrijk is, is toon het top, nou die hoogste top is zeker wat betreft privacy en informatiebeveiliging bij de les. Dat stralen ze ook uit. Dat is al één randvoorwaarde. Maar we spreken nu ook duidelijk de hele lijn aan dus afdelingshoofden en werkplekmensen op hun verantwoordelijkheid daarin. Als je het niet goed doet, dan kunnen dit de consequenties zijn. Dat vertellen wij aan die mensen. Als je daar vanuit onze rol als FG's consequent in bent, dat die mensen het ook echt begrijpen en dat het tot hun hersenen doordringt dat ze zorgvuldig moeten handelen omdat er anders ernstige consequenties kunnen zijn dan gaat het ook een stuk beter merken we'.

Inrichting informatiebeveiligingsbeleid
H1: 'Wat we ook, dat wil ik toch wel even noemen als het gaat om communicatie en awareness en dergelijke. Wij zeggen ook van privacybescherming en informatiebeveiliging moeten onderdeel zijn van de reguliere bedrijfsvoering. Dat iemand dat een beetje apart zit te oreren vanuit een ivoren toren dat werkt gewoon niet. Wat we nu aan het doen zijn is een aantal zaken. Je hebt de plan – do – check – act cyclus, dat is de sturende manier van deze organisatie waaraan eigenlijk het hele lijnmanagement aan deelneemt en daar willen wij eigenlijk ook als het ware een normaal onderdeel van zijn. Onder andere is het zo dat hebben we bijna bereikt: dat we gewoon gaan deelnemen aan de reguliere interne audits hier, dus privacy en informatiebeveiliging wordt onderdeel daarvan, dus tegelijkertijd met patiëntveiligheid en informatiebeveiliging wordt dan ook getest. Oja, één dag behandelen we al deze aspecten'.
H1: 'Een ander punt waarop we dat willen bereiken, daar zijn we ook wat laat mee, is het integraal risicomanagement, dus patiëntveiligheid, financiën, gebouwen. We hebben nu ook geregeld dat we ook onderdeel zijn van het risicomanagement van deze instelling'.
H1: 'Ja, dat doen wij nu al hè risico-inventarisatie, maar dat moet natuurlijk een onderdeel zijn van de integrale bedrijfsvoering. Waarom zijn het anders risico's? Het is gewoon weer een risico. Dus onze visie is ook maak het onderdeel van de integrale bedrijfsvoering. We zijn daar acties voor aan het ondernemen dat dat daadwerkelijk gebeurt. Je moet altijd een soort lange termijnvisie hebben, want als je dan kijkt naar hoe is het ideaal geregeld als je dan wil dat het op een zo'n onderdeel ideaal geregeld is zoals het beschreven staat en in de norm opgenomen staat dat is een heilloze weg dan verlies je meteen je geloofwaardigheid. En dan ben je in plaats van dat je een stapje vooruit maakt, ben je er tien achteruit, want mensen gaan je ook vermijden, dus je moet eigenlijk ook proberen een stap te maken waarvan je zegt ja dit is het nog helemaal niet, maar het is een stap voorwaarts. Dan weet je oja, nu deze stap en volgend jaar die stap. Dus je moet als het ware een langetermijnvisie hebben waar je uiteindelijk wilt komen. Nou heb ik nog nooit meegemaakt in mijn leven dat ik mijn doel bereikt heb dat blijft toch altijd voor zich uit bewegen, maar je moet wel een organisatie als het ware meenemen'.

Communicatie-inzet informatiebeveiligingsbeleid
Onderzoeker vraagt of H ook een intranet heeft H2 antwoordt: 'Ja, we hebben ook een intranet en ICT zet daar bijvoorbeeld ook regelmatig berichtjes op als er weer ransomware is of iets anders, maar dat wordt slecht gelezen'.
H1: 'Maar de effectiviteit daar hebben wij grote twijfels over'.
H1: 'Als we kijken naar de incidenten die er dan zijn die we afhandelen, dat wij elke keer ons afvragen van 'hoe is dit nou mogelijk?''
H2: 'En als we dan vergelijken met andere organisaties die beperken dan de privacy tot de zorg, maar wij pakken dan gelijk het onderzoek mee op zo'n afdeling. Dat loopt ontzettend door elkaar heen namelijk'.

Verschillende benaderingswijze voor verschillende groepen
H1: 'Nee. Dat is wel een goede wat je vraagt nu.

Vragen van medewerkers
H2: 'Waar ik de meeste vragen over krijg is 'ja maar wat moet ik dan? Hoe kan ik het dan veilig versturen?''

H1: ‘Een veel voorkomende vraag’.
H2: ‘En anders mag dit? En dat is een andere vraag waar ik meestal mee zit: mag dit?’

Bewustwording van medewerkers
H1: ‘Ik merk wel dat als ik op de afdelingen ben, daar hadden we het vorige week ook over, dan zijn die zorgverleners zich allemaal heel erg bewust van het beroepsgeheim. Met hoofdletters en drie strepen erachter dat is er wel ingepeperd. Dat is natuurlijk op zich al heel belangrijk dat ze zich daar bewust van zijn. Maar de bepalingen die voortvloeien weer uit de Wet Bescherming Persoonsgegevens die kennen ze weer niet en de privacyaspecten zoals die opgenomen zijn daar weten ze ook betrekkelijk weinig van’.
Onderzoeker zegt dat je dan wel zou zeggen dat ze al bewustwording hebben H2 antwoordt: ‘Ja, zeker die hebben ze, maar op een gegeven moment heb je, dat vind ik wel een heel mooi voorbeeld, waar je dan specifiek in het research domein tegenaan loopt. Kijk artsen vragen altijd naar een geboortedatum en een naam om er zeker van te zijn dat je de juiste patiënt voor je hebt en dat moet ook. Maar op het moment dat je nu zegt van we gaan nu onderzoek doen dan is het eigenlijk al not done. Dan mag dat eigenlijk alleen maar gecodeerd dat je niet meer meteen weet wie het is. En die omschakeling die moeten velen nog maken, dus dat je dan dus niet naar een geboortedatum moet vragen want die heb je ook helemaal niet nodig. Heb je niet aan een leeftijd genoeg of nog beter aan een leeftijdscategorie?’
Onderzoeker geeft aan dat dat voor mensen achter de balie natuurlijk wel relevant is maar voor onderzoek niet H2 antwoordt: ‘Ja, voor onderzoek niet. Daar is het ook wel belangrijk, maar daar valt een vergissinkje, ja dat kan wel pijnlijk zijn voor het onderzoek maar ja de patiënt wordt er over het algemeen niet zieker op’.

Lastige punten om groepen te bereiken
H1: ‘Nou lastige punten om die groepen (medewerkers) te bereiken. Op zich kun je die groepen prima bereiken alleen je moet zorgen dat je hun aandacht krijgt. Hè want iedereen is hier natuurlijk heel erg druk en logisch ook dat is echt gewoon patiënten, onderzoek en onderwijs. Dit is natuurlijk iets wat erbij komt. Ze werken natuurlijk in een wetgevend kader op allerlei gebieden. Ze hebben het over corporate governance en huiscircuit en budgetten en weet ik het allemaal daar zit ook een stuk privacy en informatiebeveiliging bij, dus je moet zien dat je op een of andere manier met begrip voor waar die mensen al dan niet functioneren en waarvoor ze hier zijn. Moet je proberen op een gepaste manier aandacht hiervoor te krijgen, want de risico’s zijn wel steeds groter. Dus dat nemen we dan wel mee.

Maatregelen bij niet naleven regels
H1: ‘Nou dat is wel een goede van je. Onder andere doen we nu aan login-opvolging. Met andere woorden: ‘heb je rechtmatig toegang gekregen?’ Er is nu een complete brief in de maak, die naar iedereen gaat die vertrouwelijke gegevens moet raadplegen, die krijgen het op de deurmat. Daar staat ook in inderdaad dat er spelregels zijn en dat als ze zich daar niet aan houden dan kan dat rechtspositionele consequenties hebben, zoals een disciplinair gesprek tot en met ontslag. De Raad van Bestuur zegt: we gaan hieraan echt consequenties verbinden’.

Risico’s in beeld bij bestuur
Onderzoeker geeft aan dat de Raad van Bestuur de risico’s dan waarschijnlijk al goed in beeld heeft en vraagt wat zij dan als specifieke risico’s zien voor deze instelling H1 antwoordt: ‘Heel goed. Nou natuurlijk het onrechtmatig raadplegen van gegevens. In zijn algemeenheid geldt hè als je kijkt naar de risico’s waarvan ze zeggen: ojee daar komt ellende uit. Op nummer 1 staat met stipt het gebrek aan awareness waardoor mensen in kennis gehinderd fouten maken en daardoor incidenten veroorzaken. En waarvoor wij eigenlijk nog het meest beducht zijn dat is reputatieschade’.
H1: ‘Dat is voor zo’n organisatie, een gezondheidsorganisatie, is dat het allerbelangrijkst’.
H1: ‘Wij zijn ook opportunistisch hoor. Als er een incident is dan kijken wij wat er ook alweer op ons lijstje staat en dan oja dat hoort daarbij en dan meteen zetten we dat erin als advies naar de Raad van Bestuur, want we hebben een vaste afhandelprocedure. Dus wij maken elk incident dat een beetje omvang heeft, daar maken wij misbruik van om meteen de Raad van Bestuur te laten stempelen van daar moet wat gebeuren’.

Evaluatie van incident

H1: 'Ja er is een enorme reputatieschade aangericht in die tijd. Dus daar zijn ze zich heel erg van bewust: 'straks word ik door mevrouw Tweebeeke onder handen genomen' Want onze Raad van Bestuur is toen natuurlijk afgebrand'.

Bijdrage van communicatie om risico's in te perken
H1: 'Nou het feit dat het ook benoemd is. We hebben net een managementreview geschreven naar de Raad van Bestuur. Dan kan de Raad van Bestuur zich een oordeel vormen hoe het hier op dit moment is ten aanzien van informatiebeveiliging, maar dat hangt samen met privacybescherming natuurlijk. En daar staat gebrek aan awareness op nummer één, dus communicatie is natuurlijk het allerbelangrijkste'.

Welke methode werkt wel en welke methode werkt niet
H1: 'Nou strategieën, als je praat over de awareness zien wij wel dat de datalekken dat dat ons enorm helpt'.
H2: 'Maar dat zijn herkenbare voorbeelden, want heel vaak wat in die wetgeving staat dat is eigenlijk alleen te abstract. En dan maak je al een heleboel vertaalslagen naar de praktijk, maar dan nog blijft het moeilijk. Dus voor een deel is het: hoe verpak je onze boodschap in iets waar mensen wat van begrepen hebben en wat blijft hangen?'
H2: 'En vaak helpt het inderdaad gewoon als je een mooie casus hebt waaraan je het kan ophangen, want dan herkennen ze het en dan kom je erin'.
H1: 'Sowieso hè nog wel een belangrijk aspect dat wil ik dan nog wel noemen. Als je kijkt naar de FG's, die zijn heel erg goed in die wet en de interpretatie van die wet en dat vind ik echt onvoorstelbaar en dat vind ik heel knap ook, maar het gaat er natuurlijk om. Je kan het beter ietsje minder weten, maar juist in het communiceren erover ook face-to-face, met mensen over praten, zorgen dat het op de agenda staat, jezelf in feite ook een beetje opdringen hè maar dan op een leuke manier, dus erover communiceren is het allerbelangrijkst. En je denkt vaak over communicatie met plaatjes, posters en al dat soort dingen en filmpjes, maar het communiceren dat de FG's dat doen, met de leiding, met het management, met de werkvloer. Erheen gaan is nog veel belangrijker. Het uitspitten van de wet en dan een hele grote Excel te maken dat je precies weet waar het verschil zit en wat er dan voor maatregelen genomen moeten worden, daar bereik je het niet mee'.
H2: 'Maar wat jij hier noemt: knelpunt. Nou één van de knelpunten is de tijd die wij zelf erin kunnen steken. Het is iets dat structureel aandacht nodig heeft en het lukt ons nog niet helemaal om daar helemaal genoeg capaciteit in te steken'.
Onderzoeker vraagt of er dan wat meer ruimte zou mogen komen of nog iemand aangesteld zou moeten worden H1 antwoordt: 'Nou dat gaat niet gebeuren, maar je moet natuurlijk proberen je netwerk groter te krijgen, mensen die daarmee bezig zijn. Dat is het enige wat op dit moment tot capaciteitsuitbreiding zou kunnen leiden, maar ik zou zelf eerder benoemen: weet je communicatie is echt een heel moeilijk vak eigenlijk om dat goed te doen en dit is iets: je kan niet zeggen we gaan één keer communiceren en dan weet iedereen het. Nee, dit heeft een soort permanente aandacht nodig en weet je het is net zo als dat je iedere avond boerenkool zou eten, dat zou heel erg gaan vervelen. Zorg dat je telkens wel iets op een andere manier doet, waardoor je mensen blijft aanspreken. En wij zijn natuurlijk vanuit ons vak heel sterk gericht op de inhoud en je wilt vanuit de inhoud je boodschap kwijt, maar omdat je zoveel kennis hebt van het vakgebied, schiet zo'n boodschap vaak ook zijn doel mis natuurlijk'.
H1: 'Ja natuurlijk, ja. We zijn natuurlijk heel trots dat we overal van die do's en dont's posters ophangen, maar ja ik weet zelf ook wel dat de effectiviteit daarvan beperkt is. We doen het alleen voor een auditer eigenlijk, een externe auditer, van kijk daar hangt ie. Nou top je hebt je in ieder geval aan die norm heb je voldaan. Maar eigenlijk willen wij wat onze visie daarop is wij willen eigenlijk echt effect bereiken. De Raad van Bestuur wil ook echt effect de Raad van Bestuur geeft de opdracht om echt effect te hebben: 'wij willen geen papieren tijgers'. Ik vind zelf die creativiteit om telkens op een goede manier mensen te bereiken, dat vind ik het allermoeilijkste'.

Evaluatie van incidenten
Onderzoeker vraagt of er ook casussen besproken worden in de organisatie of alleen bij de betreffende afdeling als er dingen voorvallen H1 antwoordt: 'De incidenten sowieso. Dat is ook verplicht. Afdelingen moeten ook verplicht melden en die vraag ik ook naar audits dan, maar sinds we de Wet Meldplicht Datalekken hebben, hebben we wel daadwerkelijk incidenten waar ook een hele hoop mensen mee aan de gang gaan en die mensen worden ook verwacht waar de incidenten ontstaan dat ze er wat mee doen en daar worden ze ook

op aangesproken. En wat wij nu willen doen en dat zei jij ook vorige week dat we deze incidenten ook gaan gebruiken als voorbeelden om de incidenten ook sprekend te maken'.

Verandering sinds invoering van Wet Meldplicht Datalekken
H2: 'Ja, er is natuurlijk ook meer aandacht aan gegeven. Ik merk zelfs bij mensen die het eigenlijk al zouden moeten weten die denken er dan niet aan. Die weten het eigenlijk wel, maar die betrekken het dan niet op hun eigen situatie. Concreet voorbeeld: iemand was met een online vragenlijst bezig en realiseerde zich opeens bij een vragenlijst besteedt je dingen uit, dus hoort daar een bewerkersovereenkomst bij. Die was daar eigenlijk ook wel van op de hoogte, maar voor haar eigen onderzoek viel op een gegeven moment pas het kwartje van oh ja dat is waar ook. Op een gegeven moment moet je daar dus iets voor gaan regelen'.

Procedure Meldplicht Datalekken
H1: 'Nou die werkt als de beste'.
H2: 'De praktijk leert dat wij meestal gebeld worden of er komt een mailtje binnen of het komt via ons meldsysteem, maar het meeste is gewoon rechtstreeks contact met ons'.
H1: 'Ja, of mensen rennen m'n kamer in. Nog even over de signalering, want dat is eigenlijk het allerbelangrijkst, wat hebben wij ingericht voor de signalering? Dat is vrij uitgebreid. Doen we even op volgorde: er kan gebeld worden, een nummer gewoon. We hebben dat mensen persoonlijk binnen kunnen komen. We hebben een meldsysteem daarin staan ook een aantal vragen naar een datalek. We hebben omdat datalekken ook op allerlei manieren kunnen binnenkomen ook verloren pc's en weet ik wat het allemaal zijn. Receptie of beveiliging neemt meteen met mij contact op als er sprake is van een gestolen laptop of een gevonden laptop of iets anders in de harde sfeer. Daarnaast kunnen ook datalekken binnenkomen via social media. Voor ons wordt permanent social media in de gaten gehouden wat erover gezegd wordt, dus zodra er sprake is van een melding of iets wat een datalek zou kunnen zijn, dat is nog nooit gebeurd trouwens'.
Onderzoeker vraagt wat ze zich voor moet stellen bij datalekken die binnenkomen via social media
H2: 'We hadden zoiets gehad er stonden röntgenfoto's van iemand die stonden op internet. Dat klopte allemaal, maar dan kan je zeggen van hee'.
H1: 'Maar ook klagende mensen van: nou m'n gegevens lagen daar en daar en hoe vind ik dat nou hè? Dus dan gaan mensen in hun omgeving via social media dingen zeggen. Daarnaast krijg ik ook iedere dag worden alle andere media, de formele media, gescreend op onze instelling. Die kijken iedere dag na of het een artikel zou betreffen waarin iets over het uitlekken van gegevens staat. Nou zijn we een tijdje geleden naar aanleiding van zo'n uitzending ook getipt door een collega dat er mogelijk sprake zou zijn van een datalek. Ik vond het te ver gaan en heb er niks mee gedaan, hij vond van wel. Maar goed dat is ook mijn beoordeling. Dat is de voorkant hè dus die wordt dichtgetimmerd'.
H1: 'Nou dus een hele korte procedure, tak tak tak tak, voor de afhandeling'.
H2: 'Je mist nog één dat is de afdeling ICT'.
H1: 'Oja ICT, sorry een hele belangrijke, de helpdesk waar ook natuurlijk van alles binnen kan komen en die melden het ook direct bij ons als er sprake is van een ernstig datalek, zoals malware of gegevens vernietigd dat is een datalek. Dan doen wij de eerste beoordeling en indien het een ernstig incident is dan nemen wij meteen contact op met de secretaris van de Raad van Bestuur dan vind er een beoordeling plaats en dan wordt gekeken of we dat in een kleine setting kunnen afhandelen. Dat betekent dat wij toetsen aan de wet en kijken of we melding moeten doen aan de AP en of betrokkenen geïnformeerd moeten worden en dergelijke en op die manier geven wij dan een advies en dat neemt de Raad van Bestuur over of niet en dan zorgen wij dat het uitgevoerd wordt, maar bij een ernstig incident, met andere woorden veel gegevens, mogelijk ook imagoschade, dat hebben we eigenlijk twee keer gehad maar daar hebben we één lek van gemaakt dan wordt het hele circus opgetrommeld. Iemand uit de Raad van Bestuur wordt de voorzitter van de beheersgroep. Daar zit ook de directeur Communicatie en daar zit de voorzitter van de commissie privacybescherming in en daar zitten wij in en daar zit de directeur ICT bij en de technical security officer die kennis heeft van de harde informatiebeveiliging, dus heel technisch'.
H2: 'En verder mensen die dan nodig zijn van de afdeling'.
H1: 'En dan komen we afhankelijk van de ernst: één of meerdere keren per dag bij elkaar zal ik maar zeggen. En dan wordt daar netjes verslag van gemaakt en we bouwen een dossier op. De procedure is eigenlijk heel kort en krachtig. Het zijn eigenlijk maar drie velletjes en dat is ook eigenlijk de kracht van de procedure: iedereen weet meteen wat hij moet doen en wij zijn eigenlijk degenen die dan het proces sturen. Dat is een hele

belangrijke rol die we hebben. Wij zijn toezichthouders en adviseurs he, dus vanuit die rol doen we dan ook dat we adviseren wie wat moet vinden, besluiten, afwegen enzovoort, dus wij regisseren dat'.
Onderzoeker vraagt of je dan naar de secretaris Raad van Bestuur gaat om het aan te geven en dan beoordeelt of het in kleinere setting of met een grote groep wordt opgelost H1 antwoordt: 'Ja, maar altijd als er sprake is van een door ons gedetecteerd datalek dat beoordelen we eerst, dan beoordelen we vervolgens of we de AP inlichten en de betrokkenen moeten informeren. Dan volgt er altijd een advies van ons tweeën want we reviewen mekaar ook. En dan gaat dat advies, ons gezamenlijke advies altijd naar de Raad van Bestuur naar een vast persoon, één voor de zorg en één voor onderzoek en onderwijs. En dan nemen ze het al dan niet over. En dan geven ze het terug en dan zorgen wij dat het als zodanig afgehandeld wordt'.
Onderzoeker vraagt of Raad van Bestuur er ook voor kan kiezen om het niet over te nemen en wat er dan gebeurt H2 antwoordt: 'Dat hangt er vanaf wat er is. Meestal is het advies wel of niet melden bij AP of wel of niet melden bij de betrokkenen. En vaak komen er ook wel maatregelen dus die stellen we ook voor'.
H2: 'Het is heel concreet ja'.
Onderzoeker vraagt of Raad van Bestuur wel uiteindelijk degene is die beslist of iets gemeld wordt H1 antwoordt: 'Ja, zij moeten, wij mogen niets wat dat betreft, zij moeten. We hebben een soort standaard rapportage staccato, de feiten. En dan krijg je soms een beetje context erbij en dan beoordelen we is het een datalek ja of nee? en dan een stukje wet. En dan moet de betrokkene geïnformeerd ja of nee? De AP?'
H2: 'Afwegingen en daar staan onze aanbevelingen dan. Want ze moeten heel snel beslissen. En daarmee stel je je ze daartoe in staat'.

Rol van de Autoriteit Persoonsgegevens
H1: 'Ja, we hebben wel informatie gevraagd niet over datalekken, maar in het kader van de interpretatie van de beleidsregels. Hoe heet dat ook alweer medisch dossier van zieke medewerkers. Nou ja in april hebben we die vraag gesteld en we hebben eind vorige maand pas antwoord gekregen eigenlijk, nog niet eens officieel maar officieus. En dat duurt heel lang en we merken wel dat dat advies van de autoriteit persoonsgegevens dat is typisch ivoren toren advies, want het sluit niet aan bij eigenlijk de praktijk. Het advies van de autoriteit persoonsgegevens van onze kant denken wij dat zij dan ook moeten kijken naar de context waarin dat advies als het ware omgezet moet worden in werkbare processen. Duurt erg lang. We kregen ook vorige week toen werd jij benaderd een paar weken geleden over een datalek van een patiënt en dat de AP dacht van welk datalek zal dit overgaan?'
H2: 'Ja, we hebben meerdere datalekken gemeld'.
H1: 'Ja een stuk of zes denk ik ook hè. Ja want we moeten ook weer verslag erover uitbrengen natuurlijk'.
Onderzoeker vraagt dat je dan dus gemeld hebt en dan een vraag van de autoriteit krijgt H2 antwoordt: 'Ja dat dacht ik maar dat ging over iets heel anders dat ging over een medewerker die had geklaagd over de procedure als je je wachtwoord vergeten bent, dan wordt het BSN gebruikt en daar had dan iemand over geklaagd. Gelukkig hadden we het zelf ook al gedetecteerd en hadden we het opgelost. Ergens in de zomer is die procedure geweest maar de klacht was al van voor de zomer'.
H1: 'Kortom ze zijn traag en als er advies gevraagd wordt is onze ervaring dat het advies nog niet aansluit bij de praktijk'.
H2: 'Nou dat het te ver weg staat, ze gaan puur van het juridisch theoretische uit'.
Onderzoeker vraagt of ze de AP toevallig al een keer gesproken of gezien hebben H1 antwoordt: 'Nee, zij spreken niet met mensen'.

Bijeenkomst van de NGFG
H2: 'Ja dat verslag hebben we wel vernomen ja. Dat ging dan over die datalekken en daar zeiden ze dat je redelijkerwijs moet kunnen uitsluiten dat. En dan begreep ik dat die persoon daar het woord redelijkerwijs schrapt. Je moet kunnen uitsluiten. Ja dat kunnen we nooit'.
H1: 'Wat we dan doen is ook gewoon, we gaan gewoon uit van redelijkerwijs, want het is onredelijk om dat eruit te halen, want dan is het altijd foute boel. Je moet daar wel bij realiseren dat als je er verantwoording over kunt afleggen naar de rechter over hoe het gedaan is dan is het wat ons betreft oké'.

Voorbereiding op de AVG
H1: 'Nou we hebben toevallig net een managementreview geschreven dat we een heel eind op weg zijn op basis van een overzicht dat is samengesteld met andere UMC's. Dus dat is wel zo'n erg handige Excel dan weten we nog precies wat we allemaal moeten doen, maar we verwachten dat we een heel eind op weg zijn.

Weet je, we hebben bewerkersovereenkomsten, we hebben de Meldplicht Datalekken, we hebben alleen bijvoorbeeld zaken nog niet als die dataportabiliteit en onze transparantie is nog niet optimaal maar wel redelijk en dan hebben we ook natuurlijk nog het cliëntenrecht in de zorg'.
H1: 'Ja en toestemming hebben om informatie te verstrekken en om informatie te krijgen en dan moet het ook nog eens een keer gespecialiseerd zijn wat dus dat zijn ook dingen die op ons afkomen. En we hebben hier natuurlijk ook een data protection officer aangesteld, twee zelfs, met bevoegdheden als zodanig met een goede positie in de organisatie. Die AVG maak ik me niet eens zoveel zorgen meer over'.

6.9 Categorisatie interview Zorginstelling I

Functie van functionaris gegevensbescherming
Onderzoeker vraagt hoe I op positie van ICT-manager terecht is gekomen (hij is nog niet officieel aangesteld als FG) I antwoordt: 'Dat komt omdat ik 25 of 30 jaar geleden als programmeur ergens begonnen ben en nooit wat anders ben gaan doen'.
I: 'Een ouderwetse ICT'er zeg maar'.
Onderzoeker vraagt hoe I bij opleiding voor FG terecht is gekomen I antwoordt: 'Nou mede door de publicaties over die nieuwe WBP en de Wet Meldplicht Datalekken dat ik dacht 'ja daar moet iemand wat over weten binnen dit bedrijf' en toen ben ik daarmee begonnen. Ik ben inmiddels daar wel na de juridische procedures ben ik daar wel mee gestopt, dus ik maak die opleiding niet af'.
I: 'Nou omdat ik dacht dat alleen het begin erg juridisch getint zou zijn, maar zij zeiden dat op een gegeven moment gaan we het over security hebben en maatregelen en weet ik veel wat en dan wordt het wat praktischer, dat zag ik niet, ik vond het niet heel praktisch worden en ik ben geen jurist. Dus ik vond het wel mooi geweest'.
I: 'Ja en wat dat betreft ben ik nu wel goed op de hoogte wat betreft de Wet Meldplicht Datalekken'.
Onderzoeker vraagt wat I zoal doet op het gebied van privacy en de bescherming van persoonsgegevens I antwoordt: 'Roepen dat het heel hard nodig is. Nee, het is absoluut niet onderkend hier dat we daar wat aan gaan moeten doen. Ik heb een nulmeting laten doen door een organisatie voor het hele bedrijf en die ligt nu bij de Raad van Bestuur en daar gebeurt niks mee op dit moment'.

Thema in beeld bij bestuur
I: 'Wel in beeld, maar ja ze acteren nog niet echt'.
Onderzoeker vraagt of I kan verklaren waarom I antwoordt: 'Waarom weet ik niet, nee, ik weet niet waarom'.
I: 'Ja, de Raad van Bestuur is er maar één dus die heeft niet eens een portefeuille. De Raad van Bestuur is één iemand. Maar de Raad van Toezicht zal dit ook op zijn agenda moeten hebben, alleen daar ligt het nog niet omdat het bestuur dat daar niet neerlegt. Maar misschien handig om te weten dat wij binnenkort een nieuwe bestuurder krijgen. Dus er zijn hier een aantal dingen die aan het veranderen zijn'.
I: 'Dus dat is onvoldoende nu'.

Belegging van de functie in de organisatie
Onderzoeker vraagt of I zich dan als enige bezighoudt met het onderwerp privacy in de organisatie I antwoordt: 'Nou dat is wel heel erg kort door de bocht. Laten we zeggen naar intensiviteit ben ik de enige ja. Maar dat neem ik allemaal mee in dat project NEN 7510, dus ik wil de komende twee kwartalen wil ik dat echt gaan uitrollen en daar gaat natuurlijk een heleboel in mee. Daar komt ook een datalekprotocol in en een commissie en vaststellen wie doet wat en wanneer en die awarenesscampagne waarin ik privacy gewoon meeneem, dus ja het gaat binnenkort wel allemaal gebeuren. Dat wel'.
I: 'Ik ben manager van de ICT-afdeling'. Onderzoeker vraagt of I dan ook andere mensen beschikbaar heeft daar die hier iets mee kunnen I antwoordt: 'Nee, nou ja dat laatste zou nog kunnen maar ze hebben geen tijd. Hier laat ik mij ondersteunen door een externe partij'.
Onderzoeker vraagt of hij er dan wel voldoende tijd voor heeft I antwoordt: 'Nou als je voldoende weghaalt dan klopt de zin'.
Onderzoeker vraagt hoeveel uur per week I ongeveer bezig is met het opzetten van het project I antwoordt: 'Dat is heel verschillend: de ene keer 10 minuten en de volgende keer dertig uur. Het is nog niet zo gestructureerd dat ik daar ook echt, kijk als dit nou gedaan is en we hebben dat managementsysteem voor de normering dan ga ik me ook weer wat strakker met privacy bezighouden, maar ja ik weet ook niet hoe de organisatie er over vier maanden uitziet dus dat maakt het niet makkelijker. Vandaar dat het toch nog een beetje mijn feestje is hier'.

Informatie over de instelling
Antwoord van I op vraag of I veel thuiszorg en veel verpleeghuizen heeft: 'Nee, geen thuiszorg alleen verpleeghuizen'.
I: 'De Raad van Bestuur is één en de directie is vier'.

Inrichting informatiebeveiligingsbeleid
I: 'Nou omdat ik ook security officer ben, ben ik ook bezig met NEN 7510 en van daaruit moeten we NEN 7510 gecertificeerd worden volgend jaar. Eigenlijk ook als een onderligger op de Wet Datalekken. Het staat er niet keihard in als voorwaarde, maar het is feitelijk wel een voorwaarde vanuit de wet, dus vandaaruit dat ik ook dingen ga doen. Maar dat is meer mijn feestje dan het bedrijfsfeestje op dit moment'.
I: 'Er is eigenlijk al jarenlang een project geïdentificeerd om dat te doen en daar hebben we nu externe ondersteuning bij ingeroepen en we implementeren een managementtool daarvoor die de auditors en de maatregelen die daaruit komen echt monitort en op regelmatige basis ook bij stakeholders neerlegt. Dus het is eigenlijk een tool waarbij je die hele NEN-norm die stop je daarin en daar maak je dreigingsanalyses en impactanalyses en daar komen maatregelsets uit en die maatregelen koppel je weer terug aan stakeholders in het bedrijf. En die tool die monitort dan de plan-do-check-act cyclus van al die maatregelen bij al die stakeholders'.
I: 'Eigenlijk elke dag één druk op de knop en een real time audit van je hele normering van het hele bedrijf'.
Onderzoeker vraagt of er nu dan wel maatregelen gedaan worden, maar de medewerkers nog niet echt worden meegenomen I antwoordt: 'Nee, zeker de zorg niet. De overheid, zeg maar, de kantoormensen die worden er eerder in betrokken dan de zorgmedewerker op dit moment. Daar wordt toch nog wel van gedacht die willen het niet, die snappen het niet, die kunnen het niet'.
Onderzoeker vraagt of er al ideeën zijn hoe je medewerkers gaat bereiken I antwoordt: 'Nee'.
Onderzoeker vraagt of I wel een reglement heeft of gedragscodes op het gebied van privacy I antwoordt: 'Ligt allemaal ter goedkeuring'.
Onderzoeker vraagt of dat dan allemaal bij de Raad van Bestuur ligt I antwoordt: 'Ja, directie en Raad van Bestuur'.
Onderzoeker vraagt wanneer I het reglement heeft opgesteld I antwoordt: 'Dat durf ik niet te zeggen, nee'.
Onderzoeker vraagt of er in het algemeen regels zijn I antwoordt: 'Ja zeker. Er is een soort ICT-reglement en er waren algemene gedragsregels, maar het is allemaal, het is er allemaal wel, maar of oud of niemand kent het of het is niet nog een keer goed afgestempeld of goed over gecommuniceerd. Het is gewoon aan alle kanten verstoft. Dus men moet gewoon weer helemaal opnieuw de molen door en worden opgefrist zowel op het gebied van privacy als op security als op informatieveiligheid, helemaal'.
Antwoord van I op vraag of er geen mensen op toezien of het reglement goed wordt uitgevoerd: 'Nee'.

Samenwerking met communicatieafdeling
I: 'Nou wat ik net zei. We gaan een bedrijf selecteren voor een awarenesscampagne en dat doe ik samen met communicatie. Ja in feite doe ik het samen met ze zeg ik maar ik ga dat stukje overdragen naar de afdeling communicatie. Hoe ze dat gaan doen laat ik graag over aan de mensen die daar verstand van hebben'.
Onderzoeker geeft aan dat I natuurlijk wel de kennis heeft I antwoordt: 'Ja, precies de inhoud is voor mij het belangrijkste'.

Bekendheid 'ZEKER' campagne NVZ
I: 'Nee, wat is dat?'
Onderzoeker geeft uitleg over 'ZEKER' campagne I antwoordt: I: 'We gaan deze maand gaan we een bedrijf zoeken om ons met een Awarenesscampagne te helpen. Dus met wat jij nu zegt dat kan ik mooi meenemen. Ik hoor daar graag meer van'.

Risico's voor instelling van een datalek
I: 'Nou wij zijn een VVT-instelling. Daar hebben we verzorgingstehuizen voor ouderen. Ja, ons grootste risico is dat er cliëntdossiers op straat komen te liggen. Ja aan de andere kant is dat ook weer niet zo'n heel groot risico. Als het gebeurt hebben we een ernstig probleem, maar de kans dat het gebeurt is niet zo heel groot. We moeten het wel zo doen'.
Onderzoeker vraagt waarom die kans niet zo groot is volgens I, I antwoordt: 'Nou ja dan moet je echt behalve de onwetendheid van de medewerkers hè zoals dat iemand een dossier uit z'n tas laat vallen onderweg of dat

iemand hier iets laat liggen op tafel. Ja ik neem aan dat het hacken van deze instelling nou niet echt prioriteit is voor hackers, snap je. Dus in die zin het interesseert natuurlijk helemaal niemand dit. Het is alleen toeval en dommigheid waar die risico's ontstaan. Maar dat is wel iets waar een awarenesscampagne heel goed op gericht moet zijn, want mensen doen maar wat hoor'.
Onderzoeker vraagt of I al te maken heeft gehad met datalekken I antwoordt: I: 'Nee, nee'.
Onderzoeker vraagt of ze bijvoorbeeld ook al gekeken hebben naar risico's voor de instelling I antwoordt: 'Ja, ja. Daar zit een risicoanalyse in en daar zit een dreigingsanalyse in'.
Onderzoeker vraagt wat het verschil daartussen is I antwoordt: 'Nou een dreiging is natuurlijk een brand is een dreiging maar dat hoeft nog geen heel groot risico te zijn, dus het is een beetje een woordspelletje'.

Risico's in beeld bij het bestuur
I: 'Nou ze zijn zich er vaag wel van bewust, maar ze denken ook dat zal mijn tijd wel doen en het gebeurt toch niet. Dat zit er wel een beetje in, maar goed dat is voor een deel wel te begrijpen, maar het is niet oké. Je moet het gewoon goed regelen en technisch zit het allemaal best op orde hoor. Ik bedoel het is niet zo dat als je hier binnen loopt dat je alles zomaar te pakken krijgt, maar het is ook niet zo dat we een bank zijn, dus er zit altijd een financiële afweging aan in wat ik wel en niet doe. Ik heb bijvoorbeeld anderhalve maand geleden de screensaver op 4 minuten gezet en dat was al een schok hoor in het bedrijf'.
I: 'Nee, daar is niemand blij mee. Dus ja als ik er dan zo'n campagne om heen zou hebben dan wordt dat voor mij ook makkelijker'.

Lastige punten om beleid door te voeren
I: 'De zorgmedewerkers. Die zijn over het algemeen toch wat lager opgeleid en een aantal van hen ook slecht in taalgebruik. Er zijn een aantal medewerkers die slecht Nederlands spreken en die moeten het toch ook snappen'.

Veranderingen in organisatie sinds invoering Meldplicht Datalekken
I: 'Nee, ze weten helemaal niet eens dat die wet er is'.
Onderzoeker geeft aan dat dat wel interessant is want in de media wordt er best veel aandacht aan besteed en dat er genoeg voorbeelden zijn van datalekken I antwoordt: 'Maar die worden nog niet heel breed uitgetrokken'. Onderzoeker vraagt wat I hiermee bedoelt I antwoordt: 'Het valt jou op en het valt mij op, maar feitelijk is er nog niet heel veel bij dergelijke gebeurtenissen gedaan en de AP heeft ook nog niks gedaan. Die heeft nog niemand op zijn vingers getikt, dus wat dat betreft doen ze ook niet veel. Ja, er is één bestuurder op zijn vingers getikt, maar dat was niet zozeer over privacy, dat was meer politiek. Daar werd men dan al zenuwachtig van. Maar niet echt op de privacy, meer gewoon in zijn algehele niet functioneren'.

Rol van de Autoriteit Persoonsgegevens
I: 'Nou die zou in mijn ogen toch wel als ze dit echt graag gedragen willen hebben ook in de bestuurskamer dan zouden ze toch wel een keer eentje op zijn vingers moeten tikken'.
Onderzoeker vraagt of dat is omdat er nu eigenlijk niet genoeg angst is I antwoordt: 'Nou ja angst is een naar woord, maar goed hoeveel besturen hebben het privacyonderwerp in hun risicobegroting meegenomen? Nou heel weinig denk ik hoor, waarom die risico's die zijn er helemaal nog niet? Nou ja ze zijn er wel maar ze zijn niet zichtbaar'.
Onderzoeker geeft aan dat het natuurlijk ook averechts kan werken als er boetes komen I antwoordt: 'Ja, maar je hoeft niet meteen met acht ton te komen. Je kan ook een aanwijzing geven en die in de krant zetten of in ieder geval een keer publiceren: we hebben zoveel datalekken gezien en bij zoveel procent van deze datalekken hebben we ook een onderzoek gestart. Maar je hoort alleen maar ja er komt een nieuwe wet en het wordt zo streng en iedereen moet wat, maar ja goed als ze bij mij in de stad zeggen je mag niet meer rechtsaf en denk erom. En je doet er niks mee dan gaat iedereen gewoon rechtsaf. Dat is de menselijke natuur'.
I: 'Ja, ze doen het toch. Als je niet handhaaft, dan moet je ook geen wet instellen. Dat is eigenlijk mijn mening'.
Onderzoeker geeft aan dat ze misschien ook wel weinig mensen hebben I antwoordt: 'Nou neem mensen aan zou ik zeggen'.
Onderzoeker geeft aan dat er wel budget voor moet zijn I antwoordt: 'Ja, klopt. Maar ja als je boetes uitdeelt krijg je ook geld'.

Rol van communicatie bij inperken risico's

I: 'Nou omdat een heleboel mensen zich gewoon echt niet bewust zijn van het feit dat als je je kantoor uitloopt en je laat alles liggen dat je daarmee een privacyrisico loopt. Dat weten ze gewoon echt niet en dat ze op de prikborden in de huiskamers gegevens over mensen als geboortedatum en weet ik veel wat allemaal het gaat gewoon ook niet echt ergens over maar het mag gewoon niet en nou ja van die dingen en je kunt wel zeggen hoe belangrijk is het? Ja het wordt pas belangrijk als iemand gaat zeuren of een klacht indient of iets dergelijks. Maar ik ben van mening dat wij ook als organisatie gewoon uiteindelijk de volwassenheid moeten hebben om aan die wet- en regelgeving te voldoen. Ja je kan wel zeggen van ik vind het niet nuttig, maar ja, dan moet je ook gewoon in je reclame-uitingen zeggen dat je dat allemaal niet wil en niet doet weet je. Wat dat betreft ben ik natuurlijk een ICT'er en het is een nul of een één'.

Bewustzijn van medewerkers
Onderzoeker geeft aan dat ze zich kan voorstellen dat er al redelijk wat privacybewustzijn is in de organisatie I antwoordt: 'Ja, maar men is zich echt niet bewust van de vergaande veranderingen die er nu zijn. Je mag niet appen, je mag geen foto's appen, je mag geen mailtjes met dossiers naar je familie sturen. En dan kunnen we met z'n allen wel vinden dat dat onzinregels zijn, ik vind dat prima, maar dan moet je dat voor dit bedrijf gewoon opstellen dat je dat onzin vindt en dat je je daarmee niet aan de wet houdt. Het mag, maar je moet het wel regelen'.
I: 'Ik zou het niet doen, maar ik vind dat je transparant moet zijn in wat je wel en niet doet. En als jij zegt ik vind het onzin ik doe niet mee met die flauwekul nou prima maar dan moet je dat wel gewoon vindbaar maken en ja het opvragen van dossiers en de procedures daarvoor het is natuurlijk een dramawet, want er zit erg veel werk aan te komen maar ja dan moet je zeggen dat doe ik niet'.

Communicatie-inzet naar aanleiding van Meldplicht Datalekken
Onderzoeker vraagt of er bijvoorbeeld wel op andere gebieden campagnes gehouden worden I antwoordt: 'Wat bedoel je?' Onderzoeker geeft aan bijvoorbeeld medewerkers informeren en vraagt of I een intranet heeft I antwoordt: 'Ja dat hebben we allemaal wel, we hebben ook gewoon een leerportaal en trainingen en dat soort zaken. Het is allemaal wel beschikbaar maar privacy en security staan gewoon niet op de agenda. Dus als het niet over zorg of over medische handelingen gaat dan is er gewoon geen interesse voor wat ik wel snap'.

Procedure Meldplicht Datalekken
I: 'Ben ik allemaal mee bezig om dat op poten te zetten nu. Protocol datalekken en het formeren van een commissie en dat soort dingen dat ben ik nu allemaal aan het doen'.
I: 'Ik ga het even voor je opzoeken. Ik weet ongeveer wel wat er moet gebeuren. Wat gaan we doen? Opleveren van het informatiebeveiligingsbeleid, de processen en documentatie het uitvoeren van de assessments en de analyses, de overdracht van kennis en kunde het implementeren van maatregelen en de controle op de naleving van de certificering en daar zit wel veel in en we hebben een nulmeting gedaan op privacy dus dat is net weer even een iets andere insteek en daar zit ook een enorme lijst aan activiteiten in, waarvan ik er wel een paar kan opnoemen. Verkrijgen van inzicht in de verwerkingen en het benoemen van eigenaren, beoordelen of er sprake is van een gezamenlijke verantwoordelijkheid, functieprofiel opstellen voor een FG, functieprofiel voor security officer, voldaan aan informatieplicht, nou ja een waslijst met activiteiten'.
Onderzoeker vraagt of dat dan uit die nulmeting kwam dat daar stappen in genomen moeten worden I antwoordt: 'Ja, en dan meer op het gebied van privacy hè, want de NEN 7510 die is best wel gericht op de security en dit is dan weer echt voor de privacy'.

Voorbereiding op AVG
I: 'Nou 2018 daar heb ik wel een goed gevoel over. Die security krijg ik echt wel rond, dus die NEN 7510 en als je de NEN 7510 geregeld hebt dan ben je ook al wel een heel eind hoor ook met privacy die maatregelen zijn toch voornamelijk organisatorisch en schriftelijk. Nou dan komen we een heel eind, maar het moet wel gebeuren'.
I: 'En er moet een FG aangesteld worden'.
Onderzoeker geeft aan dat I die functie kan gaan vervullen of iemand anders I antwoordt: 'Nou wat mij betreft ook iemand anders, want anders wordt het ook erg chaotisch, dus voor mij hoeft het niet. Lijkt me nuttiger als ik diegene ondersteun'.

Onderzoeker geeft aan dat je ze ook extern kunt inhuren I antwoordt: 'Ja, precies dat vind ik wel een heel aantrekkelijke optie. Dan zou ik wel gewoon aanspreekpunt kunnen zijn in de organisatie'.

Aandacht van medewerkers voor thema
Onderzoeker vraagt of er dan ook geen vragen van medewerkers zijn dat ze ergens mee zitten of iets op het nieuws zagen I antwoordt: 'Heel incidenteel'. Onderzoeker vraagt wat dat dan bijvoorbeeld voor vragen zijn I antwoordt: 'Nou bijvoorbeeld de vraag van een arts of die beeldmateriaal van patiënten op mag slaan en video-opnames van gesprekken en dat soort zaken dat soort vragen'. Onderzoeker geeft aan dat er dan dus wel mensen mee bezig zijn I antwoordt: 'Nou hun vraag was dan vaak meer van een technische aard en dat ik zei van nou er zit ook een privacykant aan onderschat dat niet'.
I: 'Maar het valt heel erg mee. En je moet niet onderschatten hè de buitenwereld is er ook niet mee bezig hè. Maar als ik bijvoorbeeld een medewerker zou zeggen je mag helemaal dat dossier niet mailen nou de buitenwereld accepteert dat niet. Wij kunnen natuurlijk wel heel braaf alles tegen willen houden maar ja de zorg heeft te maken met familieleden en die hebben zoiets van 'ja weetje je zoekt het maar uit met je privacywetgeving. Je moet het me nu gewoon mailen nu''.
I: 'Maar andersom ook hè. We moeten bijvoorbeeld allerlei gegevens aan de gemeente aanleveren omdat de gemeente van alles en nog wat betaalt maar dat kan niet veilig hè. De gemeente verdomd het om iets te regelen dat het wel veilig kan en als wij het niet leveren dan krijgen wij geen geld. Dat is pas krom. Dat zelfs de overheid zich weigert aan de regels te houden'.

6.10 Categorisatie interview zorginstelling J

Achtergrond van de Functionaris voor de Gegevensbescherming
J1: 'Nou onze instelling heeft al heel lang een functionaris gegevensbescherming om te beginnen. Vanaf 2011 denk ik. Nou moet ik zeggen dat de invulling toen dat is denk ik niet meer helemaal te vergelijken met hoe het nu is. En hoe ben ik hier gekomen? Ja altijd affiniteit met recht gehad, ook recht gestudeerd maar niet afgemaakt en het leek mij gewoon wel een uitdagende baan. En dat is begonnen met 4 uur in de week en nu zit ik op 8 uur in de week'.
J2: 'En als het aan mij ligt wordt het fulltime'.
J1: 'Ja, we zijn het er wel over eens dat bij zo'n grote organisatie als ons ziekenhuis, waar natuurlijk alleen maar eigenlijk persoonsgegevens worden verwerkt, er wel meer aandacht nodig is voor het hele privacyvraagstuk'.
Daarnaast is J1 projectleider binnen het bureau strategie en innovatie.
J2 is fulltime security officer, J2: 'Nou ja fulltime, 32 uur en ik werk er 40, zoiets'. J1: 'Maar officieel 32 uur. Wij zijn samen eigenlijk één FTE. En dan hebben we nog 8 uur een security manager binnen I&A, die echt dedicated voor security wordt ingezet'.

Belegging van de functie in de organisatie
Onderzoeker vraagt waar I&A voor staat J2 antwoordt: 'De afdeling Informatisering en automatisering. Dus die echt intern binnen de afdeling zorgt dat de securityaspecten mee worden genomen, dus in de change in het problemmanagement. De security manager is ook voorzitter van het CERT ons Computer Emergency Response Team'.
Onderzoeker vraagt of J1 en J2 onder die afdeling vallen, J1 antwoordt: 'Ik niet. Ik ben de verlengde arm vanuit de Autoriteit Persoonsgegevens. Mijn functie staat ook in de Wet Bescherming Persoonsgegevens beschreven, waardoor ik als onafhankelijk intern toezichthouder m'n functie heb en daardoor aan het bestuur rapporteer als dat nodig is. Ik val dus niet onder een lijnmanager of iets.
Onderzoeker vraagt of dat rechtstreeks onder de Raad van Bestuur staat J2 antwoordt: 'Ja, en dat geldt voor mij ook. Ik val onder het bestuur en dat wisselt afhankelijk van hoe de bestuurders hun portefeuille verdelen. We hebben net weer een nieuwe bestuurder kwaliteit en veiligheid dus het kan zijn dat ik toch nog over ga naar deze bestuurder, maar dat is niet helemaal duidelijk. Ik zit nu nog bij F&C als stafadviseur en ik ga per 1 januari kom ik in de afdeling kwaliteit en veiligheid'.

Thema in beeld bij bestuur
Onderzoeker vraagt of er iemand bij het bestuur aanwezig is die dit onderwerp in zijn portefeuille heeft J2 antwoordt: 'Nou alle drie doen ze het, maar ze willen het er ook niet over eens zijn wie het uiteindelijk gaat doen. Ze vinden het alle drie interessant'.

J1: 'Nou ik denk ook wel het boeiende met dit onderwerp. Het raakt feitelijk alle bedrijfsonderdelen van je organisatie. Of het nu gaat om patiëntgegevens, personeel, loongegevens of gewoon je bedrijfsinformatie, het raakt echt overal. Dus ik snap daarom ook wel de behoefte van de bestuurders om een gemeenschappelijke betrokkenheid te hebben zeg maar'.
J2: 'Nou ze nemen het wel serieus nu'.
J1: 'Je merkt dat het laatste half jaar er wel een verandering is opgetreden ook sinds de komst van de Wet Meldplicht Datalekken dat ze toch wel iets meer doordrongen zijn van 'ja dit is toch wel serious business waar we mee te dealen hebben'. En we zien daar ook wel beweging in komen en natuurlijk gaat dat allemaal niet van vandaag op morgen we zien in ieder geval dat daar een positieve tendens aan het ontwikkelen is'.
J2: 'Ze zijn bereid om ons te gaan ontzorgen met inzet van externen. Dat kost altijd weer werk, maar dat maakt niet uit. Er komt wel wat'.
Onderzoeker constateert dat ze er dus wel mee bezig zijn om het aandacht te geven J2 antwoordt: 'Ja, want ik heb nu ook een juridisch medewerkster al sinds driekwartjaar die nu afstudeert voor privacy onder andere en die doet al mijn bewerkersovereenkomsten, dat is gewoon een gigaklus en dat krijg je er echt niet bij in je uren. Dan hadden wij nu ook geen gesprek gehad'.
J1: 'Nee, maar het feit dat dat ook kan zie je ook wel dat het bestuur zich ook wel van doordrongen is van 'hee er moet daar wat gebeuren we zullen dat anders moeten gaan organiseren die vraagstukken die er al liggen en die op ons afkomen'.

Prioriteit van privacy in organisatie
J2: 'Nee, wel een hoge'.
J1: 'Het is hoger dan dat het was'.
J2: 'Het staat in het risicoprofiel van de organisatie, daarin is het ook benoemd. Ze hebben het vorige week maandag met het MT besproken en toen werd er ook nadrukkelijk gezegd van is het wel nadrukkelijk genoeg beschreven, moeten we het niet wat hoger nog op de prioritering zetten? Cybercrime staat er ook op. Dus het is de combinatie van de dreiging en wat je verplicht bent om te doen en die combinatie maakt dat men het dus hoog op de agenda heeft staan'.

Verhouding tussen privacy en de bescherming van persoonsgegevens
J1: 'Nou privacy dat vind ik eigenlijk een wat naar woord, want ja wat is privacy? De bescherming van persoonsgegevens is eigenlijk dat je de persoonlijke levenssfeer respecteert en dat bedoelen we denk ik ook met privacy als we het er zo over hebben. Dus ja volgens mij bedoelen we hetzelfde of we het nu hebben over privacy of over Wet Bescherming Persoonsgegevens'.
J2: 'En zeker als we straks naar de Europese Wetgeving gaan dan is dat helemaal helder, dat is gewoon één ding. En informatieveiligheid is een onderdeel van de norm dat is beschikbaarheid van informatie, integriteit van informatie en vertrouwelijkheid van informatie en ja wat is vertrouwelijkheid?'

Voorbeeld: In combinatie is het moeilijker om persoonsdata te herkennen
J1:' Dus de kwalificatie van je informatie maakt hoe je ermee omgaat. Dat is eigenlijk het meest bepalend en ik merk dat dat iets is wat nog niet in de genen hier zit. We snappen allemaal dat onze parels zijn patiëntendata of onze persoonsdata, maar in combinatie of verwerkt in informatie is het nog wel eens lastiger om die parel te herkennen. Dan zit ie ver weg in de schelp en dan in één keer ontdekken ze 'goh het is misschien toch wel handig als we daar dezelfde eisen aan stellen als wanneer het gewoon heel duidelijk is' Dus daar zit nog denk ik als je het hebt over het ontwikkelingsniveau of het volwassenheidsniveau daar is nog wel wat winst te behalen'.
J2: 'Ik heb volgens mij in 2011 mijn eerste beleid gegevensuitwisseling met classificatie van informatie geschreven. Dat was eigenlijk een soort van nieuw. Dat is net als dat 20 jaar terug Arbo nieuw was, is nu privacy en informatieveiligheid voor de zorgsector nieuw. Terwijl ze er wel altijd naar gehandeld hebben, alleen in begrippen en hoe je ermee omgaat dat is gewoon even een ander volwassenheidsniveau wat je gaat vragen'.

Inrichting informatiebeveiligingsbeleid
J2: 'Ja, ja, ja, we hebben allerlei beleid'.
J1: 'We hebben al heel veel beleid'.
J2: 'We hebben privacybeleid, privacyreglement, dat was er eigenlijk als eerste, waarbij we al aangaven hoe we met dingen omgingen'.

J1: 'En allerlei aanverwante zaken hè: camerabeleid, autorisatie, toegangsbeleid we hebben echt wel een hele waslijst daarover. Maar als je dan komt op jouw deel communicatie dan hebben we daar eigenlijk nog niet zoveel over'.

Communicatie-inzet informatiebeveiligingsbeleid
J2: 'Twee brochures bij indiensttreding: één over de samenvatting van de huisregels informatieveiligheid, waarvan privacy een onderdeel is. En één algemeen over wat informatieveiligheid is. Medewerkers worden gescreend. Ze zijn verplicht om een VOG aan te vragen en we gaan ervanuit dat ze een geheimhoudingsplicht ondertekenen, dus daar zit in de entree, daar zit iets van brochures naar medewerkers. En ja we hebben brochures voor patiënten bijvoorbeeld, we zetten iets op de website over onze cookies, dus we doen wel wat, maar we doen zeker niet genoeg.
Onderzoeker vraagt of het privacythema ook meegenomen wordt in overleggen in de rest van de organisatie (niet alleen bij management) J1 antwoordt: 'Ja, bijvoorbeeld vorig jaar hadden alle serviceassistenten een training. En die hebben we ook allemaal meegenomen in wat is nu privacy en dat is behoorlijk platgeslagen, maar dat zijn wel de mensen die de lakens bijvullen en het eten delen, maar die krijgen wel vragen van bezoek, van de patiënt in bed, maken we een fotootje, doen we dit, het is natuurlijk een hele kwetsbare groep in de organisatie die geneigd zijn veel te vertellen uit goedbedoeldheid, maar dat kan natuurlijk niet. Dus daar investeren we in. Alle nieuwe medewerkers, doet J2, is er altijd een introductiedag op de eerste maandag van de maand, die worden allemaal geïnformeerd over wat doen we, maar het is niet voldoende, want je merkt dat het ook herhalen is, praktische voorbeelden blijven benoemen en het is een taai onderwerp, het is absoluut niet sexy. Teammanagers die vinden het soms maar onzin, je hebt ook managers die nog steeds zeggen van 'hè nou moet dat allemaal en wat krampachtig'. Nou onze uitdaging is om niet krampachtig te zijn, maar te kijken naar hoe kunnen we wettelijke verplichtingen integreren in lopende processen zonder dat de professionals, de zorgprofessionals daar heel veel last van hebben en dat is natuurlijk de grootste uitdaging'.
J2: 'Ik doe van de week nu vier werkoverleggen. Drie bij radiologie, want die club is zo groot dan hebben ze drie kansen zeg maar om te gaan en bij revalidatie morgen en dan is de insteek vanuit de discipline ook al verschillend, want bij R&N hebben ze het over de foto's maken, bij revalidatie hebben ze het over de gegevensuitwisseling. Maar zo zitten er een aantal dingen die dan inherent zijn aan dat proces dan nodigen ze je uit en dan doen we een stukje voorlichting en onderricht en dat is een halen brengen verhaal. Want ik vertel wat over wat ons beleid is, hoe het zou moeten, waar aandacht voor zou moeten zijn en je haalt ook, want je hoort ook incidenten, je hoort ook waar ze tegen aan lopen en dat kun je weer meenemen in je beleid, dus daar zijn die werkoverleggen sowieso goed voor.
Onderzoeker checkt of dat er een pagina informatiebeveiliging op het intranet is en vraagt op welke manier gecommuniceerd is dat die pagina er is J2 antwoordt: 'Via de teammanagers'.
J1: 'We hebben ook e-learling, zit ik even net te denken, die iedereen volgt'.
J2: 'Ja, die zit nu in het LMS en die moeten ze volgen daar krijgen ze ook een punt voor, ook de leden van de medische staf. Medische staf wordt bij ons ook apart voorgelicht doe ik ook één keer per jaar minimaal. Ik word bij het dagelijks bestuur van de medische staf één keer per jaar uitgenodigd voor de vergadering. Cliëntenraad die zijn vernieuwd. Dus ik bedacht net dat ik de nieuwe voorzitter moet aanschrijven dat we daar weer een keertje langsgaan. Ondernemingsraad staat weer op m'n agenda, want die verspreiden ook informatie, dus daar moet ik ook weer iets van voorlichting en onderricht gaan doen, die mailen ook naar iedereen, dus ik dacht oja dat is weer een dingetje. Dus zo proberen we wel die communicatie goed op gang te houden'.
J2: 'Ja en het is wel grappig want ik onderteken met die 'wees alert, wees bewust, wees zorgvuldig'. En nu hadden we het wachtwoordbeleid, hadden we een aanpassing gedaan, dat we om de 150 dagen ons wachtwoord moeten wijzigen en dan hadden ze een brief gemaakt met mijn naam eronder, maar dat is een script wat dan naar 600 medewerkers tegelijk gaat en toen hadden ze dat logo er niet bijgezet. En we hebben een virus gehad en toen heb ik een mail uitgestuurd naar alle gebruikers, erop gewezen dat we het tijdelijk zouden blokkeren en iedereen voorzichtig aangegeven: 'klik niet op de phishingmail', de phishingmailactie hebben we trouwens niet aan meegedaan. Ik was op vakantie en ik was te laat met aanmelden. Maar goed nu kreeg men dus die mail met mijn naam eronder, maar zonder dat logo en dat is aanleiding geweest voor vier mensen om mij te bellen en te vragen is dit geen phishingmail want er staat een link en jij communiceert altijd met dat logo en nu staat dat er niet bij, is dit wel van jou? En toen dacht ik nou dit is winst, dat betekent dus mensen letten goed op, mensen zeggen van klopt dit wel? Ik moet nu op een linkje klikken. Dus dat betekent wel dat je die alertheid bij de gewone gebruiker dat je die wel bereikt hebt. En als ik me soms voorstel aan een gewone verpleegkundige die ik zelf niet ken of die ik ooit bij een introductie heb gezien en dan zegt ze van ja

maar ik ken je wel want ik krijg wel eens mail van jou en heb je naam wel eens gehoord of ik zie het wel eens en dan denk ik van nou ze relateert wel aan jou als persoon en de boodschap die hebben ze dan meestal toch ook wel meegekregen'.
J2: 'Nou dan heb je toch zoiets…'.
J1: 'Maar daar werk je ook al heel wat jaartjes aan'.
J2: 'Uhm, vanaf 2010 dus, ja 6 jaar'.
Onderzoeker vraagt wat voor informatie er bijvoorbeeld wordt gegeven aan medewerkers tijdens zo'n voorlichting J2 antwoordt: 'Nou ik laat een Youtubefilmpje zien van hoe makkelijk je al je informatie op internet en hoe je daarbij kan komen en dan vertel ik gewoon even de grote lijnen van wat kun jij hier zelf doen en wat doen wij, wat proberen wij ook om jou technisch te ondersteunen om het makkelijk te maken, dus bijvoorbeeld dit (laat zien hoe je in en uitlogt door enkel je pasje te scannen) dat hadden we toen nog niet en nu hebben we dat wel en dat betekent dat ik ook verwacht dat iedereen heel snel in en uitlogt'.
J1: 'Ja en dat is nog wel een puntje'.

Bewustzijn van medewerkers
J1: 'Wat ik wel mooi vond ik was vanochtend bij de fysiotherapie, want ik zag in het screen de foto van het team en toen vroeg de ene fysio aan de ander ja waarom heb je die foto van ons daar zo staan? Ja zegt die andere fysio maar anders zie je de persoonsgegevens. Dus hij logt dan niet in en uit omdat ze zoveel continu van patiënt naar patiënt gaan, maar hij zegt ik heb het zo ingesteld dat als ik er dan niet in ben dat er een screen komt van een foto van ons fysioteam en dan zie je geen persoonsgegevens. Nou toen dacht ik of het ideaal is is een tweede, maar het gaat om de gedachte en daar gaat het om. Dat is wat je natuurlijk wil dat zij erover gaan praten. Je moet ergens beginnen'.

Maatregelen bij niet naleven regels
J2: 'En dat is nog steeds een puntje. Vanochtend had hier op de afdeling een externe die werd ingehuurd haar scherm openstaan en toen had iemand haar muis omgezet van links naar rechts en iedereen eromheen wist het en zat te wachten tot ze zou exploderen omdat ze niet meer snapte wat er gebeurde. 'Ja' zei een collega 'je weet het hè, J2 zit daar en dat mag niet hè''.
J1: 'Beetje hardleers'.
Onderzoeker geeft aan dat het hier op de afdeling misschien ook iets logischer is als ze er iets mee doen J2 antwoordt: 'Nou nee hoor hier bij de afdeling was het in het begin echt een uitdaging'.

Evaluatie van incident
Als ergens een incident op een afdeling is dan is één van de sanctiemaatregelen, is altijd dat er een werkoverleg komt en dat de betrokken medewerkers daarbij aanwezig zijn. En dat bedoel ik niet heel zwaar'.
J1: 'Het is niet als sanctie, maar als leren van hè'.
J2: 'Kijk wat je doet is eigenlijk zo van laten we nou met zijn allen leren van wat we fout hebben gedaan en laten we er vooral extra weer attent op zijn, want het gebeurt heel snel, heel makkelijk, onbedoeld ook. En dat is waar mensen werken, worden fouten gemaakt en daar kun je met elkaar van leren, maar het is wel altijd een aanleiding om te zeggen van 'goh nou laten we dat dan even doen'. Plan mij in voor het eerstvolgende werkoverleg en meestal doen ze dat dan ook braaf'.

Evaluatie van beleid
Onderzoeker vraagt of dat vanuit hen kwam om langs te komen J2 antwoordt: 'Ja, ja, ja en ik let ook wel op of ik afdelingen niet heb gehad, dus ik heb nu even weer geturfd en dan zie ik dat vanuit de FB (facilitair bedrijf) niets komt. Dus dan ga ik de manager FB weer even aanschrijven en dan zeg ik van 'wat mij opvalt is dat jullie op geen enkele vorm blijkbaar iets gedaan hebben aan informatiebeveiliging, kun je mij het tegendeel bewijzen? Dat ik iets heb gemist misschien dat jullie dat allemaal zelf doen aan de hand van onze mooie pagina informatieveiligheid en privacy. Dat zou zomaar kunnen maar ik weet het niet. Dus kun je me het dan even vertellen?''
Onderzoeker vraagt of daar dan wel op toegezien wordt J2 antwoordt: 'Ja, dat hoort in onze plan-do-act-check cyclus te zitten dat we af en toe controle doen, maar ja dat is het eerste wat erbij inschiet. Maar dit soort dingen doe ik tegen het einde van het jaar voor het overzicht naar de Raad van Bestuur van wat is er nou gebeurd dan wil ik wel altijd even checken en dan zijn er wel dingen die opvallen. Bijvoorbeeld goh die afdelingen komen wel regelmatig langs en daar gebeurt ook van alles, maar daar gebeurt niks'.

Voorbeeld: radiologie voorlichting
Toevallig had ik gisteren een voorlichting bij radiologie. Ons beleid is dat er geen foto's worden gemaakt, alleen met toestemming van. Daar worstelen zij verschrikkelijk mee. Want iedere patiënt wil als die op tafel ligt in de buckykamer, wil een foto van zichzelf maken of de moeder wil dat van het kind en dat moet gelijk op Facebook en wij willen dat niet. Dus we willen dat niet om verschillende redenen: één er kan iemand op staan die daar geen toestemming voor heeft verleend, twee er kan bedrijfsinformatie op staan waarvan wij niet willen dat dat meegaat. Want die foto is niet meer alleen voor het fotoboek thuis voor later om voor het kind te zeggen van ja in die tijd lag je heel veel in het ziekenhuis kijk maar. Nee, dat gaat gelijk op internet dat moet met de hele familie worden gedeeld, dus je hebt een ander soort beleving daarbij en dat maakt het voor medewerkers soms lastig om te communiceren naar die patiënt van dat mag niet. En dan zegt die patiënt van: 'Ja wat een onzin waarom mag dat dan niet dat is toch mijn eigen foto? En als je het dan uitlegt dan snappen ze het ook wel, maar eigenlijk is er heel veel weerstand tegen, dus toen zei één van de medewerkers van 'kunnen we geen posters ophangen met: foto's maken dat doen wij?' Ja, dat vonden wij een hele leuke, dus die heb ik ook meteen opgeschreven dus daar gaan we denk ik ook wel over nadenken om daar medewerkers van radiologie bij te helpen, maar misschien ook wel op de spoedeisende hulp'.

Bekendheid 'ZEKER' campagne
J1: 'En we hebben meegedaan met de Alert Online campagne'.
J1: 'Hebben we ook met een kraampje bij het restaurant gestaan met folders en informatie en noem maar op en daar hebben we ook iedereen geattendeerd op de community en ga daar eens naar toe en daar zijn leuke vragen uit gekomen en foldertjes meegegeven, dus zo proberen we het steeds te verbreden eigenlijk'.
J1: 'Een kraampje van ons en dat hadden we gewoon strategisch neergezet dat als je ging eten dan kon je niet om ons heen eigenlijk. En dan was het natuurlijk nog wel aan degene om wel of niet aan te haken bij dat kraampje. Maar kijk wij kennen veel mensen in het ziekenhuis dus je kan ook met een lolletje wat makkelijker van 'hee heb je dit al gezien of hoe doen jullie dit?' Je kan wat ontspannen iemand betrekken bij het onderwerp zonder dat je met een opgeheven vinger gaat staan'.
J2: 'Kijk dit was ons standje. Dit is onze bestuurder en dit is de security manager van I&A'.
J2: 'En we hebben ook in die week heel veel blogs geschreven, bijna dagelijks. Hebben we blogs geschreven aan de hand van het thema van de NVZ, de week van de privacy heb ik mensen op geattendeerd dat dat op televisie kwam'.
J2: 'Ja dat is hier is dan de nieuwspagina. Hier hebben we ook gestaan zeg maar (wijst op bovenstuk websitehomepagina) dus nu komen er alweer verschillende andere artikelen en daar zag je ons ook langskomen'.
J1: 'En je hebt ook een tijdlijn. Dan popt het daar ook op en dan kan je ook reacties doen en dingen'.
Onderzoeker vraagt of ze ook meegedaan hebben met de 'ZEKER' test J2 antwoordt: 'Zeker zorg die? Drie mensen. Met een goede uitslag hoor. Het is grappig dat je maar drie man nodig hebt om het beeld te bevestigen dat je zelf hebt. Klinkt niet valide, maar het was wel zo. Het verbaasde mij echt. Er kwam uit dat wij de eerste twee punten niet goed hadden en dat klopt ook. Weetje het beleid is bekend dat is er allemaal wel'.
Wie stelt beleid op
J2: 'Nee, de Raad van Bestuur keurt alleen maar goed'.
J1: 'Nou jij bent de grootmaker zeg maar van beleid en daar waar het kan maak ik ook beleid maar dat druist natuurlijk feitelijk in tegen mijn functie'.
J2: 'Zij helpt me er alleen maar mee'.
J1: 'Maar ja weet je als je maar één FTE hebt die dat moet faciliteren, ja dan ga je roeien met de riemen die je hebt. Dat is eigenlijk het verhaal'.
J2: 'Maar we hebben als ziekenhuis een heel goed netwerk en we maken dankbaar gebruik van elkaars stukken. Nou was ik wel één van de eerste die stukken schreef zeg maar binnen het vakgebied. Maar daar zijn al heel veel varianten op gekomen en er zijn ook mensen die weer iets doen wat ik nog niet had gedaan, dus ja daar doen we het betere jatwerk. Want we zijn allemaal vaak projectmedewerker of maar een halve FTE, dus het is nogal een zwaar onderbemande functie voor het werk dat er ligt'.

Risico's voor instelling van een datalek

Onderzoeker geeft aan dat een datalek niet te voorkomen is J1 antwoordt: 'Nee, zeker niet als het van buitenaf is. Kijk van binnenuit kan je natuurlijk heel veel doen want dan is het veel gedrag. Dan heb je het toch over voorlichting, mensen bewust maken'.
J2: 'Ja, met die foto hebben we het gewoon echt niet gezien. Dat was ook iets de proefdruk op het beeldscherm was anders dan de druk op papier, waardoor je op de papierenversie met een vergrootglas de patiëntgegevens kon lezen, terwijl ze het gecontroleerd hadden op het scherm en ja dan kun je zeggen van wat slecht, maar dat heeft echt met nog weer scherper bewustzijn te maken van dat het er daar dan toch weer anders uitziet dan dat het hier op papier staat en dat iedereen tegenwoordig een vergrootglas op zijn telefoon heeft zitten en dat je dat dan ook kunt zien. Mensen met goede ogen kunnen dat ook zien'.
J1: 'Ik vind wel dat met die nieuwe privacywetgeving op een bepaalde manier we ook wel lijken door te slaan'.
J2: 'Ja dat vind ik ook'.
J1: 'Maar goed identiteitsfraude is wel iets dat één van de grootste risico's is van een datalek wat je moet communiceren, want dat vond ik in het begin heel lastig van wat vertel je nou aan een patiënt waarvan de data gelekt is wat het risico is? Wat is nou het risico? Dat weet je niet altijd. En soms weet je wel waar de informatie terecht is gekomen bij een verkeerde persoon of er is per ongeluk een lijstje naar een patiënt opgestuurd en die patiënt heeft het dan weer netjes teruggegeven, maar daar stonden dan vijf andere patiënten op met hun naam en geboortedatum en dat ze bij een bepaald specialisme zijn gekomen, maar goed we hebben al die patiënten netjes geïnformeerd. Dat is de communicatie daarover dat je transparant bent dat dat is gebeurd, het is echt crisiscommunicatie hè'.

Risico's in beeld bij bestuur
J1: 'Nou ze willen sowieso geen datalek, omdat je vertrouwen wilt en je imago maar je wilt ook gewoon dat er geen dingen op straat komen te liggen waarvoor het niet bedoeld is, dus het bestuur die wil gewoon überhaupt niet dat er datalekken plaatsvinden. Dat willen wij ook niet'.

Procedure Meldplicht Datalekken
J2: 'Nou ja kijk dan weten we nog niet hoe dat gaat lopen hoor. We hebben eigenlijk drie soorten meldingen. Eén gaat via de helpdesk, dat is wat er bij de helpdesk binnenkomt. Hè zoals we hebben een storing of informatie is niet beschikbaar, dus dat is ook een vorm van incident. Als de vertrouwelijkheid wordt geschonden dus er is de verkeerde mail naar buiten gegaan, dan horen we het ook via die weg dus dat zijn meldingen die bij de helpdesk binnenkomen. Dan heb je de meldingen die of bij J1 of bij mij binnenkomen en dan heb je nog de meldingen die voortkomen uit de VIM-meldingen. Dus dan ziet een VIM-commissie dat het gaat om informatieveiligheid of privacy en dan komt het ook bij ons'.
J1: 'En dan heb je nog de bron de klachten van de patiënt, dus het kan zijn dat de patiënt een klacht heeft ingediend bij het patiëntenservicebureau en dat daardoor een incident boven tafel komt'.
J2: 'Dat zijn eigenlijk de stromen die je probeert bij elkaar te brengen. En ik hoop daar volgend jaar nog een wat betere tool voor te hebben dat dat allemaal wat makkelijker met elkaar verbonden wordt, maar dat loopt er een beetje achteraan. We beginnen met excellijstjes en dan wordt het beter'.

Communicatie-inzet naar aanleiding van Meldplicht Datalekken
Onderzoeker vraagt hoe de procedure gecommuniceerd is J2 antwoordt: 'Ja op de gebruikelijke manier'.
J1: 'Ja, via het intranet, maar ook in de nieuwsbrief van de kliniek bijvoorbeeld. Vastgesteld dat het een bestuurlijk besluit is en we zitten nu eigenlijk nog in de afronding van de nieuwe versie'.
J2: 'Ja, want we hadden er al één voor de wet'.
J1: 'Ja, vooruit geanticipeerd hadden we dus ja als dat dan bekrachtigd is dan communiceer je er weer over. En ja het management die moet dan ook zijn teamleden daar weer over informeren, dus het is dan vanuit de lijn dat naar beneden moet worden gecommuniceerd nou ja en jij doet heel veel voorlichting en introductie en daar is het ook gewoon een item'.
J2: 'Ja iedere introductie zeg ik 'Meldplicht Datalekken' en als er een datalek is willen we worden gebeld, niet alleen gevimd maar ook gebeld want dan moeten we binnen een bepaalde tijd handelen en nou ja dat gebeurt ook'.
J1: 'Denken we'.
Onderzoeker vraagt of ze ook folders of iets dergelijks gemaakt hebben J2 antwoordt: 'Brochures is nog wel een dingetje'. J1: 'Brochures dat behoeft gewoon aandacht, daar moeten we echt nog wel een slag in maken'.

J2: 'Ja, daar hebben we het ook met de manager communicatie over gehad. En dat zit hem ook vooral in dat hele toestemmingsverhaal van de patiënt dat zullen we toch steeds beter en goed moeten communiceren. Dus zowel naar onze medewerkers als naar de patiënten. Ik had laatst een login van een patiënt en die was echt verbaasd dat hij ineens een nieuwe bezoeker login zag staan. En toen zei die: huh is dat een onderzoeker? En toen zei ik: Ja heeft je hoofdbehandelaar dat niet met je besproken want wij zijn een STZ-ziekenhuis en dan weet je toch dan doen we onderzoek'.
J1: 'Staat ook op de website'.
J2: 'Ja, maar daar heb ik eigenlijk nooit bij stil gestaan en dat is ook zo ik denk dat het ook zo werkt. En dat betekent dat er toch nog ondanks dat er een informed consent ligt dat je toch nog iedere keer weer extra moet zeggen'.
J1: 'En dat dwingt de AVG natuurlijk ook af'.

Samenwerking met communicatieafdeling
J2: 'Ja, we hebben een vaste medewerkster bij communicatie'.
J2: 'Nou als er een incident is of alert online en afhankelijk van wie er dienst heeft, want zij draaien ook diensten'.
J1: 'Ja maar de brochures die lopen feitelijk anders, want als er bijvoorbeeld een brochure gemaakt moet worden dan maak ik die brochure en communicatie kijkt alleen van klopt het in de juiste lay-out en that's it, dus dat moet je wel zelf doen. Communicatie maakt geen folders. Dat zullen wij echt zelf moeten doen'.
J2: 'Ja en dat maakt het dus dat ik soms denk had ik maar een afdeling communicatie die dat wel deed'.
Onderzoeker vraagt wat communicatie dan bijvoorbeeld wel doet of er bij het opstellen van beleid ook een hoofdstuk communicatie is J2 antwoordt: 'Ja, ik heb een communicatieplan dat schrijf ik ieder jaar opnieuw dat hoort in het kader van de NEN-7510 gaat ook naar de bestuurder en het ligt vast dat we bepaalde acties doen zoals alert online en daar wil ik ook budget voor, een minisymposium, brochures, e-learning dat kost allemaal geld, dus dan moet je dat begroten, dus ik laat communicatie dan een plan maken. Maar wat je ziet is dat communicatie ook een soort van in de waan van de dag leeft en dat maakt: de basis beheersdingen die hebben daar gewoon nooit een prioritering. En ik denk wel eens hoe kan ik dan ontzorgd worden door een afdeling communicatie? Is dat er iemand heel actief zegt van 'Oja, dit is jouw communicatieplan jij zou toch bloggen? Zal ik even een opzetje maken wat is je onderwerp?''
J1: 'Ja, want kijk eens hoe gebruiksonvriendelijk onze website is voor de patiënt, het is een gedrocht. En eigenlijk zou je willen dat de afdeling communicatie zegt van goh ik zie zoveel informatie ik stel voor om dat even in een andere vorm te gieten zodat het toegankelijker wordt en beter benaderbaar. Wij zijn geen communicatieadviseurs, dus wat doe je? Ik gooi het er allemaal op en dan denk ik ja dan staat het er maar, maar het klopt natuurlijk niet'.
J2: 'Ja en ik ben gewend om beleidsstukken te schrijven, maar dat betekent niet dat dat een communicatiestuk is'.
J1: 'Maar ook de aanvraagformulieren het is het allemaal net niet'.
J2: 'Dus dat is wel een worsteling kan ik je vertellen'.
J1: 'Daar hebben we gewoon hulp bij nodig'.
J2: 'En het punt is dat heb ik nu ook tegen de nieuwe manager communicatie gezegd: ik wil daar gewoon letterlijk in ontzorgd worden. Ik wil gewoon een communicatiemedewerker die uit zichzelf bedenkt hé het is november daar zit de week van de privacy in want dat heeft ze gegoogled en dat heeft ze gezien en gaan we daar wat mee doen?'
J1: 'Nou liever nog: ik heb een idee wat we zouden kunnen doen. Want nu lopen wij folders te maken, eigenlijk lopen wij alles zelf te doen'.
Onderzoeker geeft aan dat de meeste organisaties wel privacybeleid, gedragscodes en regels en dergelijk hebben J1 antwoordt: 'Ja, dat gaat niemand lezen'.
Onderzoeker vraagt of er dan bijvoorbeeld geen bewustwordingscampagnes worden opgezet J2 antwoordt: 'Nou niet op die manier, als wij het niet initiëren niet'.
Onderzoeker vraagt hoe de afdeling communicatie ligt binnen de organisatie J2 antwoordt: 'Valt ook onder de Raad van Bestuur'.
Onderzoeker vraagt of de manager communicatie in de Raad van Bestuur zit J2 antwoordt: 'Nee, die zit niet in het MT. Vroeger wel, nu niet meer. Het MT is heel klein geworden, maar de manager communicatie zit wel in het informeel overleg'.
J1: 'Ja, maar wie zit daar niet bij'.

J1: 'Ik denk dat wij wel een beetje worstelen met hoe op dit moment de afdeling communicatie is ingericht of dat nog tegemoetkomt aan de eisen die er heden ten dage aan communicatie worden gesteld. In alle vormen die tegenwoordig ook mogelijk zijn en de snelheid van nieuws en van hoe breng je nou iets dat het toch blijft hangen? Want dat is natuurlijk waar het om gaat. Kijk onze intranetpagina is leuk maar als je één dag niet kijkt dan zijn alle nieuwsfeiten al weg die zakken al naar onder, die zakken al naar beneden, dus je moet dan al naar beneden te scrollen om te kijken'.
J2: 'Ja of iedere dag kijken'.
J1: 'Ja de meesten komen daar niet eens aan toe en ikzelf ook niet'.
J2: 'En ik ben een staffer'.
Onderzoeker vraagt hoe de afdeling communicatie dan nu in elkaar zit J2 antwoordt: 'Er zit gewoon een hoofd en er zijn een paar adviseurs die stand-by zijn een soort accountmanagers voor de organisatie, dus we hebben één vaste'.
J2: 'Ja, en die anderen zijn meer voor nood als er een dienst is of als er een crisis is en dan hebben we nog een medewerkster die echt alleen maar de social media doet. Maar die doet ook maar wat iedereen aangeeft dat is niet iemand die mij gaat helpen'.
J1: 'Ik had dit weekend voor het eerst wat irritant dat nu weer die vacature voorbijkomt. En dan gebeurt er iets niet goed vind ik met social media. Als ik denk van alweer dan gaat er iets niet goed in je systeem'.
J1: Wat misschien wel goed is om te melden is dat de afdeling communicatie een tijd lang zonder manager heeft gezeten en je merkt dan hoe zelfstandig is een team dan wel of niet? Hoe gaat dat verder. Nu zit er weer een manager op en ik denk dat dit soort zorgen waar wij nu tegenaan lopen dat die door deze nieuwe manager gewoon opgepikt moeten worden. En dat hij eigenlijk met een voorstel moet gaan komen van 'joh dit kunnen we bieden binnen de mogelijkheden dit niet' maar dan is het ook duidelijk. En dan weet je wel van bij wie moet ik voor wat zijn en hoe kunnen we het vormgeven.
J2: 'Ik bedoel we hebben best creatieve ideeën waar we wel eens over nagedacht hebben, maar waarvan ik niet het gevoel heb dat ik dat kwijt kan en dat iemand het oppakt. En dat is de samenwerking. Het is helemaal niet zo gek om bijvoorbeeld eens een brief te sturen naar alle patiënten over hoe wij omgaan met hun gegevens. Gewoon een brief op de mat heel simpel. Maar dat moet je bedenken en dat moet een keer ergens op komen te staan'.
J1: 'Ja of dat je een soort algemene brief doet bij de krant'.
J2: 'Maar dat zijn dingen waarvan je dan toch hoopt en dat is dan misschien nog wel leuk voor jouw onderzoek: ik zou best zoals wij NEN 7510 natuurlijk als kader hebben voor maatregelen die we kunnen nemen, zou ik eigenlijk best een soort handvat willen hebben vanuit de communicatie en voor communicatie. Hoe kunnen wij dit domein aanvliegen en wat zouden de dingen zijn die ons kunnen helpen om de bewustwording van de patiënt en de medewerker te vergroten'.
J1: 'En je leveranciers eigenlijk'.
J2: 'Dus ik denk dat we het wel weten, dus we zijn bewust onbekwaam, want wij zijn niet bekwaam in communiceren. Daar hebben wij een specialist bij nodig en daar hebben jullie voor geleerd. Voorbeeldbrieven, gewoon handvaten. Dus dat is denk ik samenvattend. Ik denk dat we zelf al heel veel gedaan en bedacht hebben, wij waren één van de eerste met een e-learning, dus het is ook niet zo dat we daar nou in stil hebben gezeten zal ik maar zeggen. We zoeken wel naar mogelijkheden om die bewustwording te vergroten. En ja het onderwerp wordt door de media natuurlijk ook meer onder de aandacht gebracht, dus dat helpt ons ook'.

Lastige punten om beleid door te voeren
J1: 'Dus wij zoeken ook heel erg naar hoe kan je nou gewoon die zorgprofessionals aan het bed helpen dat die makkelijk maar ook op een ludieke manier want vaak denk ik dat ludiek communiceren dat blijft hangen en zo serieus dat blijft niet hangen dat is teveel en met dit onderwerp wat ook saai en taai is en noem maar op hebben wij eigenlijk iemand nodig die heel creatief van geest is die snapt waar de materie privacy over gaat en die daar een goede kwinkslag aan kan geven'.
J2: 'Want ik zou best kunnen Twitteren ook als security officer waarbij ik hopelijk heel veel patiënten zou kunnen bereiken als we dat op een goede manier zouden doen dan is dat nog niet eens zo verkeerd. Maar dan heb ik daar wel hulp bij nodig dan moet iemand zeggen van 'goh zullen we dit eens Twitteren of zullen we hier aandacht aan besteden?' En dan wil ik dat best vanuit mijn profiel doen. Ik moet bijna een cursus twitteren hebben vanuit een bedrijfssetting zoals een ziekenhuis is want ja wat doe je wel en wat doe je niet. Ik doe het liever niet dan wel, ik vind het eng om te Twitteren als security officer. Ik denk ik kan het me niet permitteren als ik een foute tweet het huis in stuur. Dus ik doe het dus maar niet. Het is een veilige keuze dat snap ik ook,

maar eigenlijk zou je willen dat ik wel die stap meemaak en dat ik ik Facebook niet want daar ben ik tegen, dus ik vind dat ik dat als security officer ook zeker niet moet doen, maar als ziekenhuis hebben we wel een Facebookpagina en daar zou ik misschien best gebruik van kunnen maken om onze patiënten te informeren. Dat we zeggen wij zijn een opleidingsziekenhuis dat betekent uw data zijn in principe alleen voor behandelaars etc'.
'We hebben een grote vergrijsde bevolking hoe gaan we daar nu mee om? Kinderen die het voor hun ouders willen regelen, vrouwen voor hun man, voor hun kinderen, kinderen die een speciale positie hebben in deze wetgeving wat wel en niet mag ik vind dat een lastige materie hoe gaan we dat nou vormgeven?''

Wat werkt wel en wat werkt niet
J2: 'De introductie, dat ben ik echt van mening, daar moet je het doen. Daar zit de kracht. Dan moet je een geheimhouding tekenen en daar staat in je bent akkoord met en dan tekenen ze dus voor iets en dan lezen ze het. En dat merk ik ook als ik die voorlichting geef dat mensen dan vragen stellen, helemaal goed dan heb je het gelezen. Maar dat is eigenlijk te weinig, want daarna gaat men mee in de waan van de dag en dan is men aan het werk en dan gebeurt het dus niet meer. Als je er in de werkoverleggen geen aandacht aan besteed wordt, wordt het niet gelezen, als het niet opgenomen wordt in de notulen, als je er niet een PowerPoint achteraan stuurt en zegt van er zitten twee leuke filmpjes in dat moet je kijken stuur hem door vooral ook met je kinderen thuis bekijken zo breng ik dat dan en dan hoop ik dat ze het ook zien en kijken. Maar dat zijn dingen die ik bedenk en die ik doe'.
J2: 'Ik denk echt als je het hebt van wat zou communicatie kunnen doen in ondersteuning van dit onderwerp? Zowel de medewerkers als naar de patiënten dus dat betekent dat je iets met die social media moet doen en via het portaal als patiënten hun informatie ophalen daar kun je ook teksten neer gaan zetten'.
J1: 'Of dat je daar al een folder neerzet dat mensen kunnen zien hoe er met persoonsgegevens om wordt gegaan. Dat mensen het aan de voorkant al kunnen lezen'.
J2: 'Ja, maar dat zijn de mensen die netjes via de DIGID inloggen in het portaal en dat kan ook nog niet iedereen'.
J1: 'Ik merk wel dat als je dan toch blogt en dan probeer ik een beetje het kopje aantrekkelijk te maken, ja dat hebben we wel geleerd. Dat je nieuwsgierig wordt, maar ik denk dat wij daar meer mee kunnen, maar dan kom je gewoon aan op het punt, wie kan je helpen om dat neer te zetten en wie faciliteert je dan een beetje ook in wat speelt er in de media?'
J2: 'Hè je zou willen dat een communicatieadviseur zou zeggen ik ben dit tegengekomen in de media zullen we daar even wat mee doen? Bijvoorbeeld alle wachtwoorden zijn gehackt'.
J1: 'Laten we op actuele dingen inspelen, maar dan heb je iemand nodig die volgt wat er gebeurt. Oh hee in dat ziekenhuis is dat gebeurt en dat is leuk dat wij er iets overheen doen hoe dat bij ons gaat'.

Voorbereiding op de AVG
J1: 'Nou ja we hebben nog een jaar hè of nou ja anderhalf en we zijn best een eind op weg'.
J2: 'We zijn best een eind op weg. We hebben een nulmeting laten doen door Deloitte voor ons privacybeleid, daar kwamen natuurlijk ook communicatiedingen uit. Eén van hun voorstellen is om privacycontactpersonen aan te stellen op de afdelingen en om met dat netwerk te gaan werken om die communicatie te verwerken. Nou dat kennen we ook al van de ERGO-users van de Key-users en weet ik het wat. Dus dat is een mooi netwerk waarvan je zegt van nou soms mensen die een incident mee hebben gemaakt, die kun je een soort ambassadeur maken voor het onderwerp en die zijn dan in een keer heel fanatiek en die mailen je ook van alles toe dus daar en ik denk dat als we dat officieel maken en we doen 1 of 2 keer per jaar een bijeenkomst met die privacy officers dan hebben we natuurlijk al een goede mogelijkheid om dat te communiceren denken wij met Deloitte gaan we dat dan nu doen, maar dat is nog zonder communicatie. Dan hebben we de communicatie die eigenlijk ook moet met onze derden waarmee wij gegevens uitwisselen: de bewerkersovereenkomsten maar ook alle kleintjes wat gewoon op een politie gebeurt daar moeten we ook nog iets mee. Dus ik dacht van ja hoe gaan we al die stakeholders nog een keer communiceren? Daar loop ik wel al een poosje over na te denken maar ik weet nog niet zo goed hoe'.
Onderzoeker vraagt of J2 met dat soort vragen dan wel bij de afdeling communicatie terecht kan J2 antwoordt: 'Ja, ik kan het stellen maar dat wil niet zeggen dat ik een antwoord krijg. Dat is wel echt zo'.
J2: 'Ja en wij gaan nu naar een nieuw CISEPD. Daar willen we een nieuwe CIS onder zetten. Dat betekent dat je hele strikte autorisatieprofielen daarop moet zetten. Dat moet je zelf leren kennen, maar je moet het eigenlijk

ook gelijk communiceren, dus je moet daar iets mee. Dat voel ik ook. Ik heb tegen de projectleider ook gezegd er moet een goed communicatieplan op'.

Bijdrage van communicatie bij inperken risico's
J2: 'Ik denk dat zij als zij een actieve rol zouden vervullen dan kunnen zij heel veel doen in de preventie en op het moment dat je een crisis hebt kunnen zij curatief gewoon goed handelen'.

6.11 Categorisatie interview zorginstelling K

De functie van Functionaris voor de Gegevensbescherming
K: 'Ik werk zelf al meer dan 20 jaar in dit vakgebied en dat is informatiebeveiliging en privacy. Deze instelling heeft vier/vijf jaar geleden een functionaris gegevensbescherming aangesteld. Daar hadden ze toen een project voor ingeregeld om dat structureel vorm te geven. Toen hebben ze die functie gecreëerd en een collega van mij in die functie aangesteld. Die collega heeft mij drie/vier jaar geleden gevraagd om hem te helpen de informatiebeveiliging en privacy beter vorm te geven in dit huis en zo ben ik in zijn team terechtgekomen. En mijn collega is kortgeleden van baan veranderd, dus ik pak nu eigenlijk zijn rol even over, maar formeel hebben we een andere functionaris gegevensbescherming. Dat is iemand die tijdelijk als interim is benoemd en hij probeert zich hierop in te werken, dus eigenlijk pak ik de taken en activiteiten over van de functionaris gegevensbescherming, omdat ik inhoudelijk degene ben met de kennis en de ervaring ook in het huis hoe we hiermee om moeten gaan'.
Onderzoeker vraagt aan K of K meer op het vlak van hoe ze er in de organisatie mee omgaan zit en degene die nu wordt ingewerkt meer op het vlak van toezichthouder K antwoordt: 'Nee, hij was tot voor kort de directeur ad interim in dit huis voor informatietechnologie en informatieverwerking en is gevraagd door de Raad van Bestuur om tijdelijk deze rol waar te nemen'.

Belegging van de functie in de organisatie
K: 'We zijn op dit moment bezig om de hele informatiebeveiliging en privacybescherming beter vorm te geven op verzoek van de Raad van Bestuur, ook in opdracht van de Raad van Bestuur en we proberen daar een duidelijke scheiding te krijgen over wat gaat nu over informatiebeveiliging en wat gaat over die toezichthoudende rol? Hoe moet je dat nou goed vormgeven en waar moet je dat nou goed beleggen? Het ligt nu beide bij de staf van de Raad van Bestuur en daar komt een splitsing in en hoe dat precies nog vorm gaat krijgen is nog een beetje onduidelijk'.
Onderzoeker vraagt of er een team van functionarissen gegevensbescherming is K antwoordt: 'Jazeker, we hadden een team informatiebeveiliging en privacy van twee man, waarbij de leidinggevende rol beide rollen had zowel functionaris gegevensbescherming als centrale coördinator informatiebeveiliging. En die twee rollen daar zie je nu dat daar een splitsing in komt want het is lastig om zowel toezicht te houden op hoe je omgaat met de bescherming van persoonsgegevens en ook proberen te regelen dat het goed gebeurt in het huis. En die CISO rol is meer hoe regel ik nu met het huis dat we die gegevens goed beschermen en de andere is doen we het wel op de juiste manier?'
K: 'Nou we hebben een aantal directies, dat is meer ondersteunend die leveren geen primaire zorg en dan hebben we een aantal divisies en die leveren echt de zorg. En dan heb je een aantal divisies waarvan je zegt die komen direct in contact met de patiënt daar komt de patiënt binnen dus interne geneeskunde, de hart en longen, dat zijn poortdivisies dus daar kan een patiënt binnenkomen en dan heb je meer ondersteunend, die wel betrokken zijn bij het leveren van zorg, maar waar de patiënt in principe niet binnenkomt bijvoorbeeld biometische genetica. Deze divisies hebben allemaal een informatiemanager en de directies hebben er ook één en die worden dan ondersteund door een ICT-coördinator en functioneel beheerders, die hun eigen taken hebben in dat hele organisatieproces: het uitrollen van de middelen en het helpen van de eindgebruikers'.

Onderscheid tussen privacy en de bescherming van persoonsgegevens
K: 'Voor mij is de brede rol ik bescherm de informatie die voor dit huis belangrijk is en één van die gegevens die we moeten beschermen zijn de persoonsgegevens, maar dat is dus heel breed. Je hebt hier discussies over van als ik de naam eruit haal dan heb ik geanonimiseerde gegevens want de naam is weg. Terwijl ik zoiets heb van ja maar wacht even uit de andere gegevens kan ik afleiden wie die persoon is. Dus het is indirect herleidbaar. Nou de CISO-rol is zeg maar heel breed van hoe bescherm ik die gegevens: wat voor maatregelen moet ik

treffen, hoe communiceer ik daarover? En de FG heeft veel meer de rol van zijn die maatregelen effectief en doen we de juiste dingen? En als het fout gaat wat leren we ervan om te zorgen dat de gevolgen voor de betrokkenen beperkt blijven? En ik richt me dit jaar eigenlijk voornamelijk op dat FG werk: hebben we het goed geregeld, wat gaat er mis en wat kan ik daarover vertellen en wat communiceer ik naar het huis om dingen te verbeteren en die CISO-rol schuif ik eigenlijk door naar iemand die meer in de IT-organisatie zit, die wel zaken oppakt en probeert daar de juiste maatregelen te vinden'.

Prioriteit van privacy in organisatie
K gaf aan dat het verzoek om informatiebeveiliging en privacybescherming beter vorm te geven van de Raad van Bestuur kwam. Onderzoeker vraagt aan K hoe zij dit thema in beeld hebben, K antwoordt: 'Het staat nu in de top 5 bij de Raad van Bestuur. Ze vinden het heel erg belangrijk en de verantwoordelijke in de Raad van Bestuur hamert er ook op bij mijn collega dat we stappen moeten maken. Wat kunnen wij nog meer doen? Hoe kan ik daar beter op sturen? We doen bepaalde dingen. De zorg heeft net de kranten gehaald met er zijn zoveel datalekken en haar vraag is van doen we het nou goed, hoe kan ik beter sturen? Nou dat is dus ook dat communiceren naar haar van wat kan ik aan haar laten zien zodat zij het gevoel krijgt van ja we gaan de goede kant op of hee ik wil bijspringen'.
K: 'Nou we hebben wel budget, maar dat ligt vooral in de divisies, dus die moeten redelijk zelfstandig kunnen opereren en als die zeggen ik heb een MRI-scanner nodig en dat is een redelijk duur apparaat. Daar kun je één van aanschaffen en geen twee. Dat zijn toch vrij dure resources die ik nodig heb en hoe is die afweging. Wat moet ik daar omheen anders regelen als ik er maar eentje heb? En dat is toch echt helemaal aan de divisie zelf want die moeten de zorg primair leveren, maar eigenlijk ben je wel verantwoordelijk. Ze moeten hun broek zelf wel ophouden. Onze Raad van Bestuur heeft een besturingsfilosofie waarbij eigenlijk heel veel verantwoordelijkheid in divisies zit, want daar hebben ze ook het beste inzicht hoe ze dingen moeten doen'.

Wie stelt beleid op
K: 'Het team dat zich bezighoudt met informatiebeveiliging en privacy stelt in zijn algemeenheid het beleid op, dus we hebben een informatiebeveiligingsbeleid en een stukje rondom privacy opgesteld en dat proberen wij steeds met nieuwe stukjes tekst en beleid te vertalen naar iets wat het huis kan gebruiken.

Inrichting Informatiebeveiligingsbeleid
K: 'Je ziet alleen dat in de zorg de mensen gewend zijn om bijna voorgeschreven te krijgen hoe zij wondbehandeling moeten doen. En dat noemen zij op een gegeven moment wat is het beleid ten aanzien van de wondbehandeling? Wanneer moet ik verschonen, pleisters plakken, verband leggen noem maar op. Als je kijkt naar informatiebeveiliging dan zeggen wij hier moet je over nadenken en dit is de richting waar je wilt komen, terwijl de zorg veel meer heeft van zo moet ik het uitvoeren. Dus daar zie je een discrepantie in het woordje beleid van wat ermee bedoeld wordt. Dus wij proberen van dat algemene kader wat wij als ziekenhuis moeten volgen, de NEN-7510, dat hebben wij verder uitgewerkt in meer concrete stappen die in het huis genomen kunnen worden van oké hoe ga je informatie beschermen? En vervolgens zijn we bezig om te kijken oké hoe gaat dit landen in al die afdelingen die dit uiteindelijk moeten uitvoeren?''

Lastige punten om beleid door te voeren
K: 'Eén van de lastige punten is dat er een heleboel wet- en regelgeving naar beneden komt vanuit de overheid en vanuit de maatschappij van hier moeten we als ziekenhuis aan voldoen. En wij komen meestal on-top-off dus er zijn al een aantal dingen ingeregeld en dan is het van 'oja daar heb je die jongens van beveiliging weer die zeggen dat het beter moet'. En dat is continu communiceren; het gaat om persoonsgegevens wat kun je er wel mee doen en wat niet, neem die afweging van kan dit wel of kan dit niet. En dat stukje is voor iemand in de zorg lastig. Want die is namelijk gewend om te horen ik moet links of rechtsaf gaan in plaats van ik moet erover nadenken. Dus we hebben algemeen beleid in Nederland e-mail is niet veilig, dus patiëntgegevens mogen niet in de e-mail, maar als de patiënt nu op een operatietafel ligt en ik moet bepaalde informatie bij die arts proberen te krijgen dan kan ik het natuurlijk wel via allerlei media bij die arts krijgen, maar het is dan niet op dit moment bij die arts, dus je kunt hem opbellen, je kunt hem smsen, maar je kunt hem ook een e-mail sturen. En dan is dus de afweging op dat moment: hoe belangrijk is het dat de arts deze informatie heeft ten opzichte van ja maar misschien verlies je wat privacy. Nou die afweging moeten ze leren maken en dat is een andere insteek, dus dat is heel veel praten met, uitleggen, toelichting geven en dit soort gekke voorbeelden gebruiken'.

Bekendheid 'ZEKER' campagne
K: 'Nou wij zijn niet aangesloten bij de NVZ, omdat wij een UMC zijn. Ik heb er wel wat van meegekregen van mijn collega die er wel naar kijkt. We hebben wel eens dat kader ook binnen dit huis een campagne gestart om een stukje bewustwording weer even onder de aandacht te brengen van nou we hebben een securityweek gehad en als gevolg daarvan hebben we ook weer een campagne van welk middel moet je wel inzetten en wat moet je niet doen? En wees bewust waar je op klikt'.

Communicatie-inzet informatiebeveiligingsbeleid
K: 'We hebben voor die campagne heel duidelijk gezegd, vanuit de directie meteen, dat er deze keer een campagne gevoerd moet worden. Jullie hebben een aantal middelen en vertel die gebruikers nou eens een keer wat ze wel en wat ze niet moeten doen, want er zitten randvoorwaarden aan het gebruik van IT en communiceer daar een keer over. En dan zie je dat dat wel een lang traject is geweest om dat in gang te zetten, maar uiteindelijk hebben ze ook gezegd: 'ja dit vinden wij belangrijk want wij hebben er ook last van'. Als IT-leverancier hebben wij in dit huis op het moment dat gebruikers te vaak op de verkeerde dingen klikken. Allemaal dingen die wij niet willen hebben en moeten verbeteren. Bestanden worden weggegooid, kunnen we weer terugzetten. Klikken op mailtjes waarvan we zeggen ja wat is dit voor mailtje? Nou dan vervolgens moet de IT-club dat weer allemaal verbeteren, dus die hadden op een gegeven moment zoiets van laten we dat nou voorkomen voordat dat bij ons zover is. En dat is dan wel weer leuk. Je leert van de fouten van anderen'.
K: 'Je ziet andere ziekenhuizen hadden op een gegeven moment ergens last van en dan was het bij ons zo van 'ja wacht even zij hebben daar last van wat gaan wij doen om te zorgen dat wij dat niet krijgen?' En dat zet iets in gang, dus we hebben nu ook vanuit de Raad van Bestuur op een gegeven moment aangegeven: jongens er moet iets komen zoals een e-learningmodule, zodat gebruikers zodra ze binnenkomen die module kunnen volgen zodat ze in ieder geval de basis kennen'.
Onderzoeker vraagt aan K of er op dit moment al gesproken wordt op afdelingen over dit thema en of het op d agenda staat K antwoordt: 'Voor zover ik weet wel'.

Communicatie-inzet naar aanleiding van Meldplicht Datalekken
Eind vorig jaar zijn we begonnen met wat moeten we allemaal doen rondom de Meldplicht Datalekken. Op dat moment hebben we met z'n tweeën gezegd ja we moeten via de Raad van Bestuur gaan communiceren met het huis, dus we hebben wat teksten gemaakt voor de Raad van Bestuur. Dit komt eraan en wij verwachten dat wij dit en dit gaan doen als huis. Als er iets mis is, meld het aan bij ons. We hebben vervolgens gezorgd dat er een aantal systemen ingericht zijn en dat er een mailbak is gekomen zodat mensen informatie kwijt kunnen als 'hee ik heb iets gezien wat niet klopt'. Die pak ik op dan bel ik de mensen op om samen met de mensen te kijken wat is er aan de hand? En om dan vervolgens te zeggen is dit wel of niet een datalek en wat ga ik daarmee doen? In dat kader hebben we ook de eerste helft van het jaar zijn we zelf de organisatie ingegaan met presentaties in de afdelingen bij MT's van de divisies om te vertellen wat is nou informatiebeveiliging wat betekent privacy en wat moet je nou doen als iets niet goed gaat? En wat zijn de vuistregels? Wat doe je wel en wat doe je niet? Zo hebben we ook een aantal divisies die dit zelf opgepakt hebben, die hebben we in het begin meegenomen en gezegd: 'Ja dit kost ons veel tijd kunnen jullie helpen?' Nou een aantal zeiden nou jullie doen dat en deze heeft gezegd: 'wij pakken dit op'. En die hebben gewoon twee medewerkers dedicated op dit stuk gezet en die gaan dus bij hun eigen divisie langs alle afdelingen om te vertellen wat er aan de hand is met informatiebeveiliging, wat je moet doen om tot een selectie te komen van de juiste maatregelen en hoe je een risicoanalyse uitvoert. Betrek de mensen van centraal erbij omdat dat de experts zijn. Medewerkers komen vervolgens terug met vragen vanuit de presentatie en wij halen de antwoorden erbij van wat kan wel en wat kan niet. Dat communiceren we terug en dat wordt weer meegenomen in zo'n cyclus. Dus je ziet dat er nu heel veel aandacht wordt besteed in deze divisie aan het moet beter.
K: 'Wij hebben het eerste half jaar geventileerd van jongens we willen graag wat vertellen over dit onderwerp. We hebben het MT benaderd, de Manager bedrijfsvoering die dit in zijn portefeuille heeft, en gezegd: 'u kunt zelf een presentatie geven of wij komen toelichting geven in een teamoverleg'. En zo hebben we met zijn tweeën tien – vijftien afdelingen langsgelopen en mijn collega heeft er ook nog een aantal gehad, dus zo hebben we een aantal divisies bestookt met presentaties om dit tussen de oren te krijgen en je ziet ook dat dat soort divisies heel actief bezig zijn om na te denken over informatiebeveiliging en we hebben ook vanuit een aantal van die meldingen gezegd van wacht even we zien hier iets dat niet klopt in dit proces. Waar zit die

verstoring eigenlijk? Dan kom je erachter dat er iets ergens niet klopt, een tabel klopte niet, en als je dat dan oplost dan zie je dat het aantal meldingen terugloopt, dan heb je dus de goede actie genomen'.

Procedure Meldplicht Datalekken

K: 'Ja, we hebben een procedure ingeregeld. Op zich is het heel eenvoudig het zijn ook een paar hele simpele stappen. De persoon die het ziet kan het bij ons melden via een aantal kanalen ze kunnen mailtjes sturen, ze kunnen ons opbellen, ze kunnen het melden in het incidentmeldingssysteem. Wij pakken de meldingen dan op, nemen contact op met die mensen, bepalen vervolgens met de informatiemanager van die divisie wat er nou specifiek aan de hand is en kijken vervolgens wat er moet gebeuren. Wij voeren de coördinatie op het hele traject om te kijken of wij de juiste dingen hebben gedaan. Melden we op tijd bij de Autoriteit Persoonsgegevens, melden we op tijd bij de betrokkenen, hebben we het goed voor elkaar en kunnen we daar ook bijspringen?'

Onderzoeker vraagt of de Raad van Bestuur daar ook een rol in speelt K antwoordt: 'Nou wij zijn feitelijk staf van de Raad van Bestuur, dus eigenlijk doen wij dat namens de Raad van Bestuur. En dat is een vrij eenvoudige beslissing vind ik op het moment dat er persoonsgegevens bij betrokken zijn meld je in ieder geval bij de AP en als het dan ook nog persoonsgegevens zijn die niet adequaat zijn beveiligd ga je dus ook nog eens een keer naar de betrokkene'.

K:' Voor die datalekken zijn wij het centrale aanspreekpunt dus dat komt primair eerst bij ons en dan gaan wij het verspreiden want het kan zijn dat incidenten wel door de ene worden gezien, maar voor een hele andere divisie zijn. Nou dan weten wij op een gegeven moment ook wel van deze persoon van divisie A heeft het gezien en dit moet dus naar divisie B of naar de directie, dat kan goed gebeuren en dan proberen wij een beetje te coördineren. En dat gaat soms nog wel eens mis, dat wij denken van oh dat hoort bij die divisie en dan blijkt het toch een verhuizing te zijn, waarvan je dan plotseling zegt van oh wacht even het ligt bij een andere'.

K: 'Nou daar zijn we wel mee bezig om dat in te regelen, maar de UMC's die proberen dat gezamenlijk te doen en tot één systeem te komen, zodat we met zijn allen op dezelfde wijze responsible disclosure gaan invoeren. Ik weet wel dat wij op een gegeven moment een aantal berichten hebben gekregen van mensen die zeiden van hee dit is ons opgevallen wat moeten we hiermee en we hebben een CERT-team en ik heb gezegd: 'CERT-team willen jullie dit verder uitzoeken? Ik ken deze persoon niet. Neem contact op. Ga kijken wat er aan de hand is en ik hoor het graag''.

Onderzoeker vraagt of er een aparte vereniging is voor UMC's K antwoordt: 'Ja, dat noemen ze de NFU, Nederlandse Federatie voor UMC's. Vanuit die koepel heb je helemaal onderaan twee special interestgroups die zich bezig houden met informatiebeveiliging en privacybescherming'.

Risico's van een datalek

K: 'Als je gewoon goed kijkt naar het ziekenhuis dan denk ik dat de belangrijkste verstoringen eigenlijk de stroom zijn en nog de ondersteuning. Je hebt daar natuurlijk wel de maatregelen voor, maar we hebben stroomstoringen, storingen in de infrastructuur en dat patiënten hier niet meer kunnen komen dat zijn voor ons de dingen waarvoor je maatregelen treft. En als je dan gaat kijken naar ondersteunende informatiesystemen dan hebben we een aantal kernsystemen die mogen eigenlijk niet uitvallen. Het registratiesysteem is eigenlijk helemaal niet zo belangrijk, maar zorgen dat medewerkers weten waar ze moeten zijn als de dag begint als de planning overhoop ligt dan staan ze allemaal in de gang dan weet je niet wat je moet doen. Dus op die manier kijken we van wat zijn voor ons nou kritieke systemen en hoe gaan we dat implementeren? En dan kom je met de maatregelen. Dus afgelopen twee drie jaar zijn we ook echt bewust bezig geweest met het doorvoeren van veel meer risicoanalyses en de divisies bewust maken van oké hoe maak je die inschatting? En dan komen ze dus inderdaad met een nieuw systeem: hoe gaan we het gebruiken? Hoe ga ik het inzetten? Wat voor soort informatie komt erin? Kun je zonder deze informatie of heb je die continu nodig? En zo maak je inschattingen: nou dan zijn dit maatregelen die je kunt treffen en dan is het vervolgens aan de divisie om die keuze te maken van hoeveel geld wil ik daar uiteindelijk voor betalen'.

Onderzoeker vraagt naar meer externe gevolgen bijvoorbeeld als iets in het nieuws komt hoe ze daar dan als organisatie mee omgaan K antwoordt: 'Nou we hebben wel incidenten gehad en dat hebben ze hier redelijk voortvarend opgepakt. Ook in de communicatie van ons van wat wel en wat niet dus daar zijn ze dan wel vrij goed mee bezig. Daar hebben we dan ook een afdeling marketingcommunicatie voor die de regie vormt van als er wat gebeurt hoe gaan we daarmee om? Dan hebben we ook wel ons lesje geleerd uit voorgaande trajecten.

Er komt behoorlijk veel druk op de medewerkers en dan is het nog steeds de vraag was het terecht of niet. En dan heb je daar onderling wel discussies over, die discussie blijft natuurlijk altijd wel gevoerd worden. Ik heb ook in de buitenkant gezeten, daar wordt ook altijd geroepen: altijd melden. Dus ik meld liever en dan haal ik dingen terug dan dat ik het niet doe. Maar er zijn inderdaad ook wel situaties dat de patiënt zelf iets aangeeft en dat is eigenlijk het moment dat ik wel in aanraking kom met de patiënt. Dat ze bij mij aankomen en vragen ja ik wil eigenlijk iets van het ziekenhuis en dat is via de normale paden niet gelukt, maar wat kun jij nu betekenen voor mij? En dan komen ze soms met hele vreemde eisen. Dat bijvoorbeeld wordt gezegd: 'mijn gegevens mogen met niemand gedeeld worden' of 'nee je mag mijn BSN niet gebruiken, je mag dit niet delen, je mag mijn naam niet weten'. En dan snap ik dat ze dat willen, want dat recht mag je hebben, maar helaas heb ik ook een aantal andere eisen en ik moet gewoon een aantal dingen vastleggen en registreren in het kader van die andere toezichthouder. Als ik bijvoorbeeld niet vastleg wat ik jou heb toegediend hoe weet ik dan of ik voldoende heb toegediend? Dan hebben ze gesproken met de artsen en afdelingshoofden en dan komen uiteindelijk bij mij van ja maar kun jij dan niet iets regelen voor me'.

Verschillende benaderingswijze voor verschillende groepen

K: 'Dat wisselt vrij sterk. Dat is afhankelijk van hoe een divisie er zelf mee om wil gaan. Er zijn bijvoorbeeld divisies die zeggen van doe voor ons een presentatie of een stukje tekst, maar we hebben een website waar we intern op kunnen publiceren, we hebben nieuwsbrieven die we kunnen publiceren met daarin: jongens dit speelt, dus hou daar rekening mee. En dan proberen we een beetje in te spelen op de actualiteit dat we zeggen van hee dit speelt en dan komt er een nieuwsberichtje en dan is dat soms vanuit de directie IT, omdat het wel handig is als zij dit doen, want gebruikers die hiermee werken kijken eerder bij hen dan bij ons'.

K: 'Gewoon de IT-organisatie die zegt: 'We hebben hier last van, werk even op een andere manier of gebruik de noodprocedure om iets voor elkaar te krijgen'. En dan zie je dus dat de divisies daar vrij snel en makkelijk mee om kunnen gaan. Daar halen ze de informatie vandaan. En soms is het ook zo dat ze die informatie gewoon niet kunnen vinden. We hebben ook een centrale afdeling marketing en communicatie, die wij voor twee dingen kunnen inzetten. Heel direct en persoonlijk gericht op de persoon: de medewerker, de patiënt, de student of veel meer algemeen naar de kranten toe, de pers. En dat zijn ook weer twee vormen die je kunt inzetten'.

Samenwerking met communicatieafdeling

K: 'Nou de campagne zoals die nu loopt bij de directie IT dat is in samenspraak met de marketingadviseur en zij heeft het traject getrokken. We hebben gezegd van nou jongens dit gaat over communiceren met, niet ons vakgebied, wij zijn vakidioten. Dus jij snapt hoe je moet communiceren, zoek de juiste weg, vraag aan ons de inhoud, dan kunnen wij dat wel op die manier voeden. Dat heeft zij redelijk goed zelf binnen haar directie opgezet samen met de specialist gezegd: 'Dit is de boodschap die wij willen overbrengen'. En ze heeft dus een aantal dingen gemaakt die hier ook uitgedeeld zijn. Je ziet ze ook elektronisch, dus je kunt het nog opzoeken op het intranet'.

K: 'Het zijn niet echt folders het is zo'n geplastificeerd a4tje met een aantal spelregels erop met wat doe je wel en wat doe je niet. En die zijn door het huis verspreid en het is ook op de website geplaatst zodat medewerkers het daar vanaf kunnen halen en er zijn nog wat andere stukken tekst daaromheen neergezet om dit stukje bewustwording neer te zetten'.

Veranderingen sinds invoering Meldplicht Datalekken

K: 'In zijn algemeenheid gezegd er zijn iets meer dan 4500 datalekken gemeld. In de zorg zijn er iets meer dan 300 gemeld en als ik een beetje kijk hoe wij als huis acteren steken wij met kop en schouders boven de andere huizen uit. En niet omdat wij zo slecht of goed zijn, maar de bereidheid om hier meldingen te doen en met vragen te komen van hee wat doe ik nou goed? Is dit nu wel of niet een datalek? Ik krijg denk ik wekelijks wel vijf tot tien vragen met betrekking tot hoe moet ik bepaalde dingen doen of ik krijg een verzoek om bepaalde gegevens aan te leveren, mag ik dat wel?'

K: 'Ja, medewerkers echt vooral op de werkvloer die daadwerkelijk dingen moeten doen die komen met vragen hee maar wacht even ik doe het zo, kan dat eigenlijk wel? En: kan ik het anders doen of kan ik het beter doen? En dat is echt toegenomen'.

Lastige punten om groepen te bereiken

K: 'Ja, het is niet zozeer de locatie waar ze werken maar wel het specialisme. Je ziet dat er bepaalde divisies zijn die zijn zo bezig met een aantal grote trajecten om verbeteringen door te voeren dat ze zeggen: 'dit kan ik er nu niet bijhebben'. Daarnaast 'ik maak bijna alleen maar gebruik van standaardmiddelen dus als die standaardmiddelen goed zijn beveiligd dan hoef ik me niet zo druk te maken'. En zo heb je ook divisies die heel flexibel werken continu nieuwe dingen willen hebben en die zeggen: 'ja maar ik heb zoveel veranderingen, ik raak het overzicht kwijt. Kom me helpen om al die kleine dingetjes op orde te krijgen. Dus je hebt twee uitersten eigenlijk: degene die zegt als de techniek het maar doet dan is het oké vind ik want onze mensen werken zo weinig met informatie. Terwijl degene die contact heeft met de patiënten informatie moet uitwisselen over hoe ga je om met medicijnen die je gebruikt: moet het meer moet het minder? Of de mensen die chronisch hier langskomen dus regelmatig op bezoek komen, die wil je tussendoor ook kunnen informeren en daar hebben we een patiëntportaal voor. Dat hebben we juist gedaan om die communicatie naar de patiënt beter te maken en hij is veiliger dan alle andere manieren van communiceren, dus je ziet dat we daar eigenlijk gezegd hebben: hoe gaan we nu dat contact tussen patiënt en medewerker zodanig verbeteren dat we A effectiever zijn, dus dat het niet te lang duurt, maar dat het ook nog veilig is. En zo zie je dat als voorbeeld een traject waarbij de patiënt één keer per maand of één keer per zes weken terugkomt. Die vaste momenten komt hij terug, die verzamelt gedurende de periode zijn gegevens en in de bespreking zegt hij dit is er gebeurd in de afgelopen periode. Maar er wordt nu door artsen gezegd met de huidige stand van de techniek kan dat eigenlijk dagelijks of wekelijks, dan kan ik veel eerder ingrijpen, dus wordt gekeken naar een oplossing, maar dan wordt ook gezegd dat het wel veilig moet. Dat formuliertje kan de patiënt vergeten en dan krijg je wel een recapitulatie maar dan ben je niet volledig, dus je moet eigenlijk zorgen dat de integriteit en volledigheid van die gegevens beter wordt. Je zou het via de e-mail kunnen sturen, maar het zijn patiëntgegevens, dus liever niet via de e-mail, hoe dan wel? Dan krijg je daar dus dat er meer iets wordt gebouwd specifiek voor deze patiëntengroep waarbij je zegt ja en het is ook nog veilig'.

Maatregelen voor medewerkers bij niet naleven regels

K: 'Ja, het ergste is als ze op straat komen te staan. Dus we hebben gewoon een sanctiebeleid of medewerkers bewust dingen doen die ze niet mogen doen, dan wordt vanuit de zorg gezegd hee wacht even dit zijn wel patiëntgegevens je was niet betrokken en je hebt wel zitten kijken we gaan afscheid nemen'.

Evaluatie van incidenten

K: 'Voor zover ik ze kan overzien, want ik zit namelijk niet direct in dat stuk, omdat ik zelf ook zeg ik wil geen patiëntgegevens zien. Ik wil eigenlijk niet weten wat er gebeurd is op het moment dat je gaat kijken of er iets vreemds is gebeurd dan zit ik meestal met de artsen om de tafel en dan blijkt meestal dat het systeem of de rapportage niet klopt en dat het toch gerechtvaardigd is. Op het moment dat het niet gerechtvaardigd is dan wordt het een gesprek tussen de behandelend arts en de medewerker en dat kan weer leiden tot ontslag. Maar dat is weer privacygevoelig voor de medewerker dus dat wil ik niet weten. Dat is voor mij heel duidelijk. Er zijn een aantal van dat soort no-go's waarvan ik zeg daar wil ik niet komen'.

Voorbereiding op AVG

K: 'Ik denk dat de hele zorgsector daar in zijn algemeenheid een groot probleem heeft, omdat je twee toezichthouders hebt: je hebt de inspectie gezondheidszorg en je hebt de autoriteit persoonsgegevens. IGZ stelt een aantal eisen waar je qua privacybescherming heel moeilijk aan kunt doen. Als je de kwaliteit van zorg wilt garanderen dan moet je ervoor zorgen dat informatie beschikbaar is. Aan de andere kant zegt de Autoriteit Persoonsgegevens: nee, alleen als jij de behandelend arts bent mag je bij de informatie. Nou die twee die staan op gespannen voet, want we zijn een UMC dus als een patiënt wordt behandeld, delen wij de informatie met de directe specialisten. Nou die zitten niet aan bed van de patiënt, dus de autoriteit zegt dat mag niet, maar de IGZ zegt het is voor de kwaliteit van de behandeling wel zo goed, want die mensen geven een stukje intervisie op deze patiënt en wat hier aan de hand is en die hebben een stukje ervaring die ze inbrengen waardoor de kwaliteit toeneemt. Daarnaast hebben we hier toch de bijzondere gevallen dus het zijn meestal multidisciplinaire behandelteams dus voor je het weet heb je in bepaalde trajecten 70 verschillende specialisten nodig, dat loopt gigantisch op'.

K: 'Nou als je in het behandelteam zit dan ben je direct betrokken bij de behandeling, maar het is veel meer van 'hee ik heb hier een patiënt en denk eens mee'. Voorbeeld we lopen hier met honderd cardiologen rond, daarvan komen misschien maar vijf aan bed met een normale dienst, maar die vijf willen wel met die andere vijfennegentig sparren over dit specifieke geval, want hier is iets bijzonders aan de hand. Want een normale

patiënt kan ook in de regio behandeld worden, maar juist omdat het daar niet helemaal lukt komen ze hier. Dus het zijn wel bijzondere gevallen waar je alle kennis wilt mobiliseren die aanwezig is. Die 95 cardiologen komen dus niet aan tafel, maar die worden wel gebruikt als klankbord van doe ik als arts de juiste dingen? Nou IGZ zegt dat is toch wel nodig en AP zegt nou eigenlijk niet. Dat blijft lastig'.
K: 'Ja precies, dat gaan zij niet doen. Ze hebben vanuit het huis dat beter vormgegeven van zo werkt het en dat is getoetst tegen de Autoriteit Persoonsgegevens en die hebben gezegd dit is voor ons voldoende in ieder geval beter dan de andere huizen, maar er zitten nog punten van verbetering in. Dus je zou kunnen zeggen ik ga dat begrip behandelteam beter definiëren, zodat de toezichthouder op persoonsgegevens beter weet wat wij precies doen en dat IGZ ook zegt van wij snappen ook wat jullie doen. Dus voor een deel is het een stukje communicatie van hoe werk je met dit soort patiënten?'

Rol van de Autoriteit Persoonsgegevens
K: 'Nou ik heb wel eens geprobeerd om de autoriteit zo ver te krijgen dat zij gingen sparren. Spiegelen van: 'jongens als we het zo inregelen is dat dan goed?' En uiteindelijk was het antwoord: 'ja maar we zijn geen kwaliteitsinstituut, we toetsen aan het eind of jullie iets goeds hebben gedaan de afgelopen periode''.
K: 'Je krijgt ze niet als adviseur mee'.
Onderzoeker vraagt of K contact met hen heeft opgenomen om vragen te stellen K antwoordt: 'Nee, ze hebben op een gegeven moment een aantal onderzoeken gedaan in de zorgsector om te kijken hebben we het hier goed gedaan en toen zijn ze toevallig ook hier gekomen. En toen hebben we daar een aantal vragen neergelegd en hoe hebben we het gedaan. Nou uit dat onderzoek blijkt dat er één instelling in Nederland is die het regelt zoals de Autoriteit Persoonsgegevens dat wil en dat is een heel specifiek geval, dat is volgens mij een GGZ-instelling en daar was het op een bepaalde manier geregeld dat je inderdaad kon zeggen ja dit specialistisch stuk van zorg kun je op deze wijze inregelen. Dan heb je inderdaad een band tussen de behandelaar en de patiënt, dat is een één op één relatie. Als ik dat hier bij een harttransplantatie moet doen dan valt die patiënt op aan het eind van het behandeltraject. Want ja de ene na de ander die mag komen en die mag controleren bij een harttransplantatie ja dat gaat niet werken. Je hebt ze allemaal nodig en het liefst tegelijkertijd, dus dat is wel een spanningsveld. Het is wat overtrokken het voorbeeld maar dit is wel de discussie waar het om gaat'.

Twee toezichthouders: IGZ en AP
Onderzoeker geeft aan dat duidelijker moet worden hoe de twee toezichthouders beleid voor zich zien K antwoordt: 'Ja, maar dat is iets wat wij vooral vanuit de zorg denk ik duidelijk moeten proberen te maken aan deze twee toezichthouders'.
Onderzoeker vraagt hoe het dan zit met gemeentes, omdat deze groep ook veel informatie wil hebben K antwoordt: 'Dat weet ik gelukkig niet, want in dat stuk zit ik zelf niet. Gemeenten zitten op een andere plaats in de zorg. Wij werken vooral als tweede lijn, dus huisartsen en regioziekenhuizen besteden hun moeilijke patiënten aan ons uit. Vanuit ons gaat weinig informatie naar gemeenten voor zover ik dat kan overzien. Wel heel veel met zorgverzekeraars en huisartsen en andere kleine instellingen, maar meestal als tweede lijn achter die jongens'.
K: 'Ja, dus wij geven wel als de patiënt is behandeld een stuk informatie in de vorm van een brief dat gaat terug naar de verwijzend arts, dus die wordt op deze wijze door ons geïnformeerd. Dit hebben wij met uw patiënt gedaan'.

Informatie voor patiënten
Onderzoeker geeft aan dat ze zich kan voorstellen dat het juist van belang is voor patiënten om bepaalde informatie op te slaan in ziekenhuizen K antwoordt: 'Ja, dat klopt. De meeste patiënten die bij mij aan de deur komen die zeggen ik heb iets gezien en ik denk dat dat beter kan en ik wil graag meewerken. En kun je me helpen om dit voor mekaar te krijgen? Want artsen zeggen op een gegeven moment van ja maar dit is te moeilijk ik kan dat niet ik snap dat niet. Ze zijn heel goed als arts, maar dit is een ander onderwerp. Het staat niet primair op de lijst van dit moet ik oplossen, nee daarvoor hebben ze een concernstaf om dat te doen'.
K: 'Ja, we hebben een algemene folder voor patiënten en daarin staat gewoon beschreven wat kan ik als patiënt verwachten en hoe gaan wij om met hun gegevens. Wat kun je wel verwachten en wat kun je niet verwachten? En bij een aantal dingen staat gewoon duidelijk uitgelegd van heb je vragen dan kun je daar naar toe en heb je klachten dan kun je daar naar toe. En we hebben dat patiëntportaal dus je kunt vrij direct zien wat wij vastleggen over jou als patiënt en daar kunnen ze zien wat heeft de arts vastgesteld'.

6.12 Categorisatie interview zorginstelling L

De functie van Functionaris voor de Gegevensbescherming

L: 'Mijn functie is oorspronkelijk beleidsadviseur Zorg en Kwaliteit. Ik ben hier acht jaar geleden begonnen met de opdracht om de HKZ-certificering te begeleiden en te coördineren en daarnaast ben ik ook verantwoordelijk voor de AOIC (Administratieve Organisatie en Interne Controle). Dit heeft alles te maken met de inrichting van jouw zorgadministratie. Mijn rol daarin is om ervoor te zorgen dat alle productie zodanig gecontroleerd wordt dat we dat ook aan de accountants kunnen voorleggen, zodat zij daar een stempel op kunnen zetten. Dat is in oorsprong mijn functie. Van daaruit ben ik steeds meer inhoudelijke projecten gaan trekken zoals het invoeren van zorgprogramma's en zorgpaden. Eigenlijk toen die verplichting kwam dat we nu met informatiebeveiliging aan de slag moeten. We willen daarvoor ook voor certificering gaan. Toen is die vraag eigenlijk ook bij mij terecht gekomen, omdat ik van oorsprong gewoon projecten op mijn bordje heb die een soort kapstokkarakter hebben, dus vandaaruit kwam ik naar voren. En ik heb mijn collega informatiemanager geholpen dat op te zetten. Onderzoeker vraagt hoeveel uur L met deze functie bezig is per week L antwoordt: 'Nou officieel hoor ik hier twee dagen per week mee bezig te zijn, maar ik denk dat ik eerder zit op vier uur'.
Onderzoeker vraagt van wie het idee kwam om de functie in te voeren L antwoordt: 'Oorspronkelijk van ons Hoofd Bedrijfsondersteuning, want die zat er echt bovenop en die heeft het bespreekbaar gemaakt bij de Raad van Bestuur en zo is het gaan rollen'.

Inrichting informatiebeveiligingsbeleid

We hebben de NEN-7510 gepakt en gekeken wat de normen zijn. En wat moeten wij nog doen als instelling om daaraan te voldoen? De eerste stap die we vervolgens hebben gezet is beleid ontwikkelen. En wat we eigenlijk niet wilden doen is er een apart riedeltje voor ophangen, dus we wilden zoveel mogelijk aansluiten bij het kwaliteitsmanagementsysteem dat we hebben vanuit de HKZ. Dus informatiebeveiliging is daar gewoon een onderdeel van geworden en we hebben gekeken van nou oké wat is ons beleid ten aanzien van informatiebeveiliging. Hoe kijken wij er tegenaan? Wat vinden wij informatiebeveiliging? Wat vinden wij belangrijk? En van daaruit zijn we verder gaan kijken naar de inrichting. En dat is eigenlijk anderhalf jaar geleden dat we daarmee zijn begonnen'.

Prioriteit van privacy in de organisatie

L: 'Ja, als ik heel eerlijk ben: het heeft niet de hoogste prioriteit nee'.
L: 'Nou ik kan de Raad van Bestuur en het MT wel meekrijgen, maar als je naar de praktijk kijkt, de werkvloer dan is dat bijzonder lastig om zo'n taai thema ook ingevoerd te krijgen. Want waar zij zich op de werkvloer druk over maken is mijn productie, de patiëntenzorg dat staat bij hen gewoon voorop en daar worden ze ook op aangestuurd. En dan komt informatiebeveiliging echt op een lager prioriteitsniveau te staan, dat is nog even duwen en trekken inderdaad'.
Onderzoeker vraagt of het bijvoorbeeld wel op agenda's staat van teamoverleggen L antwoordt: 'Nee, sterker nog het veilig incidenten melden dat zou een vast agendapunt moeten zijn binnen teamoverleggen, maar daar komen ze niet aan toe joh. Ze zijn gewoon meer met de dagelijkse dingen op de werkvloer bezig dan met dat soort thema's'.

Belegging van de functie in de organisatie

L: 'Informatiebeveiliging daar is de voorzitter Raad van Bestuur portefeuillehouder van. Het hoofd bedrijfsondersteuning is gedelegeerd opdrachtnemer en mijn collega informatiemanager die is degene die het project leidt binnen de instelling en ik ondersteun daarbij'.
L: 'Nou daar zit ook nog iets tussen, je hebt Raad van Bestuur, bestuursbureau, dat zijn de ondersteunende diensten en je hebt dan het stafbureau en je hebt het bedrijfsbureau dat zijn de staffers en dan in de lijn heb je dan drie RVE's, dan heb je de directies en dan heb je de managers en dan ga je naar beneden en wij zitten aan de zijkant. En ik zit in het stafbureau en mijn leidinggevende is het hoofd van het stafbureau en die valt onder Raad van Bestuur'.
Onderzoeker vraagt of er in het stafbureau van alles zit L antwoordt: 'Ja, we zijn met verschillende portefeuilles bezig op het gebied van zorg en kwaliteit. Dan moet je denken aan cliënttevredenheid, medicatiedwang en drang. Wij zijn zeg maar echt de beleidsmakers samen met de managers en de lijn daar zitten de uitvoerders die gaan het implementeren'.

Informatie over instelling
L: 'Nee, we hebben geen thuiszorgmedewerkers. We hebben wel twee teams die mobiel zijn en naar patiënten toe gaan en dan doen we een soort outreachende zorg, maar het merendeel zijn het medewerkers die gewoon hier op locatie werken'.

Informatiebeveiligingsbeleid
L: 'Dan gaat het echt specifiek om de organisatie. Wie is verantwoordelijk waarvoor als het gaat om informatiebeveiliging? Wat is de rol van de Raad van Bestuur? Wat is de rol van de directie? Wat is de rol van de informatiemanager? Wat is de rol van de security officer? Maar ook wat is de rol van de lijn? Als zij iets signaleren wat niet goed gaat waar kunnen zij dat aankaarten. Dat is eigenlijk wat we in kaart hebben gebracht en beschreven. En wat we daarnaast hebben gedaan is kijken naar je hele IT-landschap, je hardware, je netwerk, je software, je applicaties. Als je kijkt naar de applicaties met name, wie is daar applicatie-eigenaar van en hoe verhoudt dat zich weer tot de besluiten die op dat punt moeten worden genomen als het gaat om wijzigingen of nieuwe applicaties aanschaffen. Dus de hele organisatie om informatiebeveiliging heen dat is in kaart gebracht en beschreven'.
Onderzoeker vraagt of dat een soort risico-inventarisatie is L antwoordt: 'Nee, dat is de volgende stap die we hebben gedaan. We hebben eerst het beleid beschreven wie is waarvoor verantwoordelijk. We hebben daarna alles wat wij vonden dat te maken had met informatiebeveiliging in kaart gebracht en op basis daarvan hebben we vervolgens een risicoanalyse uitgevoerd van oké waar zitten wat ons betreft de grootste dreigingen en op basis van die dreigingen hoe groot is de kans dat een bepaald risico voorkomt? Op basis daarvan hebben we een risicoanalyse uitgevoerd'.

Lastige punten om beleid door te voeren
L: 'De veelheid aan dingen die gedaan moeten worden. Je ziet als GGZ-instelling word je bijvoorbeeld door een inspectie op de hielen gezeten. Je wordt door zoveel externe organen gevolgd en gemonitord en je moet aan zoveel externe eisen voldoen, waardoor het soms zo veel is dat we eigenlijk door de bomen het bos niet meer kunnen zien en dan wordt het gewoon te veel. En dan sneuvelt een onderwerp als informatiebeveiliging, want de andere zorginhoudelijke onderwerpen die zijn gewoon belangrijker. Nou sterker nog de financiële onderwerpen zijn belangrijker. Ik bedoel als wij onze productie niet halen, het geld niet binnenkomt, dan houdt het op als we geen nieuwe cliënten hebben. Daar worden onze behandelaren op gedrild en gestuurd dat ze de productie moeten halen en nieuwe cliënten moeten binnenhalen'.
L geeft aan dat het lastig is om aandacht te krijgen voor informatiebeveiligingsbeleid.

Risico's van datalek
L: 'Nou ons grootste risico zit aan de zachte kant. Informatiebeveiliging heeft twee kanten een harde kant en een zachte kant. En de harde kant hebben we vrij goed ingericht denk ik. We hebben een deel van onze IT ook geoutsourcet en daar ook allerlei afspraken gemaakt met de leverancier. Maar wat je ziet is je kunt je netwerk, je applicaties, wel goed beveiligen, maar als mensen zich daar niet aan houden bijvoorbeeld aan wachtwoorden, aan autorisaties, dan kom je ook niet ver. Die zachte kant dat is nog een risico wat ons betreft en dan kunnen het gewoon menselijke fouten zijn waardoor gegevens op de verkeerde plek terechtkomen of gegevens op de verkeerde plek worden opgeslagen of dat men zich gewoon niet bewust is van de afspraak dat je bijvoorbeeld niet je inloggegevens aan iemand anders mag afgeven, dus dat is wat ons betreft nu toch het grootste risico'.
Onderzoeker vraagt wat belangrijke dingen zijn als je kijkt naar meer externe gevolgen L antwoordt: 'Ja, dan heeft het toch te maken met het feit in hoeverre ons netwerk beveiligd is en wat ik net al zei dat hebben we geoutsourcet en met hen hebben we gewoon afspraken gemaakt dat zij dat goed monitoren en moeten volgen en wij zitten met hen structureel om de tafel om te kijken wat er uit hun controles komt of zij dingen tegenkomen waar wij iets mee moeten'.

Bekendheid 'ZEKER' campagne
L: 'Nee, ik heb dat niet meegekregen. Wat we wel hebben gedaan, we hebben vanuit onze koepelorganisatie GGZ-Nederland, die heeft ook zo'n awarenesscampagne opgezet, waar verschillende instellingen aan kunnen meedoen als ze dat willen. En daar zijn we nu wel mee bezig om naar het materiaal te kijken van hee is dat iets wat wij ook kunnen gebruiken en willen wij in dat traject meegaan?'

Communicatie-inzet naar aanleiding van Meldplicht Datalekken
L: 'Communicatiebeleid zo specifiek niet op het gebied van informatiebeveiliging, maar we zijn wel aan het nadenken hoe we die awareness bij medewerkers op gang kunnen krijgen. Hoe kunnen we mensen bewustmaken? Want informatiebeveiliging is gewoon een ver van hun bed show, maar de kunst is om het zodanig te vertalen dat het ook voor hen herkenbaar is. Bij ons hebben we te maken met patiëntenzorg dan komen behandelaren heel snel bij dossiervoering. Wat mag je van een dossier wel of niet meegeven aan een derde? Hoe ga je met autorisaties om? Mag je inloggegevens wel of niet verstrekken aan een ander? Als je op een scherm zit en je hebt een dossier openstaan laat het niet onbeheerd achter. Dus we zijn naar de awareness aan het kijken. We hebben een e-learning ontwikkeld daarvoor, die mensen kunnen gaan volgen. Dat is denk ik iets van drie uur dat ze dan een aantal vragen kunnen doorlopen, maar echt de campagne zelf die moeten we nog gaan opstarten'.
L: 'Ja, het is maximaal drie uur dat het in beslag neemt, maar we hebben geen periode eraan gekoppeld met en dan moet het gedaan zijn. Het is gewoon als er tijd voor beschikbaar is dat ze dat moeten gaan doen. En zolang ze dat niet hebben gedaan zie je dat ook niet in het systeem geregistreerd zeg maar'.
Onderzoeker vraagt wat er in de e-learning staat en wat medewerkers leren L antwoordt: 'Nou die dingen die ik net al noemde bijvoorbeeld als je je computer hebt openstaan en er staat een patiëntdossier open en je verlaat je kamer: mag dat? Dat soort dingen staan daarop: autorisaties, wachtwoordbeleid, hoe vaak moet je wachtwoorden wijzigen? En dat je wachtwoorden niet op een papiertje opschrijft. Dat soort onderwerpen komen erin naar voren'.
Onderzoeker vraagt of de e-learning zelf ontwikkeld is L antwoordt: 'Nee, we wilden dat wel, maar dat zou gewoon veel te veel tijd in beslag nemen, maar nee dat hebben we niet zelf ontwikkeld'.
L: 'Ja en volgens mij als je de verschillende e-learnings naast elkaar zet dan zullen de thema's ook elke keer terugkomen, want daar gaat het ook eigenlijk om'.
Onderzoeker constateert dat er dus wel gedragsregels zijn en vraagt hoe medewerkers deze gedragsregels tot zich kunnen nemen L antwoordt: 'We hebben alle documentatie op het gebied van informatiebeveiliging gelinkt aan het kwaliteitsmanagementsysteem. En voor het kwaliteitsmanagementsysteem moet je al je beleidsafspraken op papier hebben staan, zodat mensen dat kunnen vinden en kunnen zien wat wij daar als instelling over afgesproken hebben. En we hebben daar een kwaliteitshandboek voor en die is opgedeeld in verschillende domeinen: zorg, organisatie, personeel, facilitair en kwaliteit en als ze dan naar de boomstructuur gaan dan kunnen ze bij facilitair zien hee informatiebeveiliging, daar kunnen ze alle documenten vinden die relevant zijn voor ze en dat kunnen ze gewoon lezen. En die gedragscodes staan bijvoorbeeld onder personeel en daar staan alle personeelsbeleidsvraagstukken in en ook de gedragscodes die ze daar kunnen vinden'.
Onderzoeker vraagt of dat hetzelfde is als intranet L antwoordt: 'Ja, dat is hetzelfde. Dat is een onderdeel van intranet. Dus als ze intranet opstarten dan kunnen ze daar gemakkelijk naar toe om documenten te vinden'.

Veranderingen in organisatie sinds invoering Meldplicht Datalekken
L: 'Nee, medewerkers zijn er totaal niet mee bezig. Nee, dat staat echt nog in de kinderschoenen. Wij proberen dat wel voor te bereiden en te ontwikkelen, maar medewerkers op de werkvloer als je die zou vragen, dan denk ik nee'.

Procedure Meldplicht Datalekken
L: 'Wat we hebben gedaan, en dat is eigenlijk ook onderdeel van de NEN-7510, is het melden van incidenten. Dat hebben we wel gecommuniceerd. Daar hebben we wel een procedure voor opgesteld. We hebben een a4 opgesteld van incidenten die bijvoorbeeld en ook weer aan de hand van die vaste thema's: wachtwoordenbeleid, autorisatie, phishing, internet als je rare dingen in je e-mail tegenkomt. Dan hebben we een a4 opgesteld en gezegd als je rare dingen tegenkomt meld het dan. We hebben een veilig-incidenten-melden-systeem en daar hebben we informatiebeveiliging een onderdeel van gemaakt. Dus als mensen bijvoorbeeld bij de printer een dossier met gegevens van de patiënten zien liggen dan moeten ze dat gaan melden. Dan komt dat bij mij, de informatiemanager en bij de manager van degene die het heeft gemeld en dan wordt dat geanalyseerd en dan kijken we van hee hoe komt het nou dat dat kan gebeuren? En zo proberen we dat wel langzaamaan bespreekbaar te maken'.
L: 'Dan is het aan de manager om te beoordelen samen met ons of het een hoog risico incident is: wat zijn de gevolgen ervan? En als dat zo is dan moet op Raad van Bestuursniveau worden besloten wat we daaraan gaan doen. En als het iets is dat bijvoorbeeld ligt aan een menselijke fout of dat het een eenmalig iets is dat probeer je dan samen met elkaar in te schatten. En als het bijvoorbeeld te maken heeft met het feit dat de medewerker

niet op de hoogte was van een bepaalde instructie, dan wordt het alsnog met het team besproken. Dus dan probeer je het met het team zelf op te lossen dat die fout daarna niet meer kan voorkomen'.
Onderzoeker vraagt of er al meldingen aan de autoriteit gedaan zijn L antwoordt: 'Niet naar de autoriteit, wel gewoon intern hebben we meldingen gehad. Dus dat zie je wel gebeuren dat sinds we dat hebben ingevoerd in het systeem dat mensen wel meer gaan melden. Dus mensen worden zich bewuster van het feit oké ik mag niet zomaar gegevens verstrekken of bij de printer gegevens achterlaten of dingen op je bureau laten slingeren, daar worden ze zich wel steeds bewuster van'.
L: 'Van alle meldingen, ook zorginhoudelijke meldingen, worden rapportages gemaakt, halfjaarlijks, je hebt maandelijkse rapportages en je hebt ook halfjaarlijkse rapportages en die worden standaard in het MT besproken. Dan wordt gekeken naar de bevindingen van hee wat zien we nou? De trend wordt besproken en dan ook eventueel de maatregelen die daarop genomen moeten worden. Dus dat wordt op dat niveau besproken met de Raad van Bestuur erbij'.

Communicatie-acties naar aanleiding van Wet Meldplicht Datalekken
Onderzoeker vraagt hoe het opgestelde a4tje is overgebracht naar de medewerkers L antwoordt: 'Via de lijn. We communiceren altijd beleidsafspraken via de directie. De directie communiceert dat naar de managers en de managers moeten dat met hun team bespreken'.
L: 'Ja, dat gaat in vaste overleggen. We hebben een overlegstructuur. Eén keer in de maand hebben we bijvoorbeeld het MT, daarna hebben we de eigen RVE's (Resultaat Verantwoordelijke Eenheden). We hebben drie RVE's dan wordt het in het MT van de RVE's besproken en daar zitten alle managers bij en die horen dat met hun eigen teams te bespreken in hun eigen werkoverleg'.
Onderzoeker vraagt of het niet zo is dat het centraal gecommuniceerd wordt L antwoordt: 'Ja, dat doen we ook. We volgen dan de lijncommunicatie, maar we hebben ook een intranet waarop we berichten plaatsen en dat doen we dan ook regelmatig, maar ja niet iedereen leest intranet, dus je bereikt denk ik echt een minimum aan medewerkers die dat dan gaan lezen'.
L: 'Nee, we hebben geen posters. Het enige dat we toen hebben gedaan is de berichten op intranet. We houden een FAQ bij en that's it. Voor de rest hebben we er geen grote communicatiecampagne aan gehangen'.

Vergroten van awareness
Onderzoeker vraagt of er al ideeën zijn over het opzetten van een campagne L antwoordt: 'L: Nee, wat ik net al zei we zouden bij een campagne van GGZ-Nederland kunnen aansluiten om te kijken of we dat kunnen gebruiken. Aan de ene kant wil je geen grote campagne opzetten, omdat het iets van de mensen zelf moet worden, dus het moet niet een apart iets worden. En wat ik net ook al zei: je moet het herkenbaar voor ze maken en als je het herkenbaar voor ze maakt dan slaat het vaak beter aan dan als je daar een hele campagne voor gaat opzetten. Dus daar zijn we nog even naar aan het zoeken van ja wat is wijsheid? Willen we daar echt bijeenkomsten voor organiseren waar ze allemaal naar toe moeten gaan? Dat daar presentaties en workshops over plaatsvinden. Of wil je dat in de bestaande overleggen en structuren en systemen gaan uitrollen? Dus dat zijn vraagstukken waar we nog mee zitten'.
L: Ja en wat je dan wel ziet is dat mensen zich langzaamaan wel bewust worden ervan.. Het sijpelt wel maar het is niet dat ze zeggen van hee en nu gaan we het zo doen.

Samenwerking met communicatieafdeling
Onderzoeker vraagt of er een communicatieafdeling is L antwoordt: 'Ja, je hebt Raad van Bestuur en je hebt daar een bestuursbureau met de bestuurssecretaris en communicatie valt onder de bestuurssecretaris'.

Maatregelen voor medewerkers bij niet naleven regels
L: 'Maatregelen worden pas genomen als ze zich niet houden aan de gedragscode, die hebben we ook opgesteld voor informatiebeveiliging. Er is nu één incident geweest waarbij een medewerker een device had waarop ook patiëntgegevens stonden wat niet mocht en daar zijn wel maatregelen voor uitgezet'.

Voorbereiding op de AVG
L: 'Nou het is de bedoeling om begin 2017 op te gaan voor certificering en ik vrees dat we dat niet gaan halen'.
L: 'Ja, voor HKZ hebben we jaarlijkse audits die uitgevoerd moeten worden door een externe decaan en zij zouden voor ons ook de NEN-7510 gaan auditen, waardoor wij ook op dat gebied gecertificeerd zouden zijn. En ik was eigenlijk ermee bezig om dat voor januari te gaan inplannen, maar dat gaan we niet halen. We moeten

nog zoveel voor awareness voorbereiden en uitrollen, dat gaat hem niet worden. Dus nu zijn er plannen om het misschien voor de zomer nog te doen en desnoods is het maar een nulmeting. Nou trouwens die nulmeting hebben we al gehad. Maar dan een eerste audit om te kijken van voldoen we nou eraan of niet en vandaaruit gaan we dan vervolgens bepalen hoe we verder gaan'.
L: 'Er heeft wel een nulmeting plaatsgevonden ja'.
L: 'Zij hebben eigenlijk geconstateerd dat we goed op weg zijn. Er waren een aantal aandachtspunten als het gaat om de toegang tot applicaties. Dan had ik een specifiek iets over authenticatie. En we moesten nog het een en ander doen op het gebied van die risicoanalyse dat mocht wat uitgebreider, dat hadden we vrij globaal en snel in elkaar gezet. Dus dat was één van de aandachtspunten en we moesten nog wat beter met onze leveranciers afspraken maken en niet alleen onze leveranciers, maar ook onze financierders aan wie wij gegevens verstrekken dat zij zich ook bewust zijn van de verantwoordelijkheid die zij hebben als wij gegevens uitwisselen. Dat zijn de belangrijkste punten geweest. En dat zijn allemaal punten die we nu hebben opgepakt en die risicoanalyse die hebben we nu gedaan dat is nu af. En die awareness dat is eigenlijk de volgende stap die we nu willen gaan zetten'.
L: 'Dat is ook een extern bedrijf die daarvoor is ingehuurd'.
Onderzoeker constateert dat de volgende stap nu is om met awareness aan de slag te gaan L antwoordt: 'Ja, en als je dat hebt gedaan dan kun je zeggen we gaan voor de zomer op voor certificering en dan is het gewoon rond'.

Rol van de Autoriteit Persoonsgegevens
L: 'Nee, eigenlijk sinds die hele functie in het leven is geroepen, die functie voor functionaris voor de gegevensbescherming, je krijgt een brief dat het moet. Ik mis dan soms een verdieping daarvan. En dan word ik dat, maar dan moet ik me ook verdiepen in al die materie en wat er precies speelt. Ik bedoel ik wil het wel serieus nemen. En dan mis ik dat van oké we moeten aan een bepaalde eis voldoen, maar ik moet vervolgens wel zelf gaan zoeken wat ik moet doen om daar te komen zeg maar. En ik denk dat heel veel instellingen dat hebben dat ze daarmee zelf aan de slag gaan en nu later. Twee jaar later bijna starten ze een awarenesscampagne en dan denk ik ja jongens dat hadden we veel eerder kunnen bedenken met elkaar, dat hadden we gewoon met elkaar kunnen neerzetten en nu zijn we allemaal individueel bezig ermee'.

Bijlage 7 Losse analyse interviews

7.1 Analyse zorginstelling A

Actieve betrokkenheid van het bestuur
De manier van betrokkenheid van het bestuur bij zorginstelling A is vrij passief. A geeft aan dat de vragen en ideeën binnen het thema privacy meestal vanuit de privacycommissie geregeld worden. De brieven die A de organisatie stuurt en de rapportages datalekken gaan wel langs de Raad van Bestuur. Ook is er een bestuurslid dat privacy in zijn portefeuille heeft. Het bestuur wordt dus wel betrokken bij het privacybeleid, maar neemt niet actief deel aan het opstellen, uitvoeren en bijstellen van het privacybeleid. Zorginstelling A probeert veel dingen in de lijn te beleggen, omdat daar ook de verantwoordelijkheid ligt.

Prioriteit van privacy in organisatie
A geeft aan dat de Raad van Bestuur natuurlijk wel ingestemd heeft met het oprichten van de privacywerkgroep en met het aannemen van A als extra functionaris voor de gegevensbescherming, dus dat er in die zin wel enigszins bewustzijn is. In die zin kan dus wel gesteld worden dat privacy prioriteit heeft in zorginstelling A. Ook is er één bestuurslid dat privacy in zijn portefeuille heeft en die dat op zich ook wel belangrijk vindt. De andere bestuursleden hebben daar iets minder feeling mee. A zegt: 'Je hebt sowieso met zoveel mensen te maken, de één vindt het heel belangrijk, de ander vindt het irritante onzin'. Op bestuursniveau is er dus wel prioriteit van privacy, maar A geeft ook aan dat er ook bestuursleden zijn die minder feeling hebben met het onderwerp en dat de één privacy wel belangrijk vindt en de ander niet. Het zou dus nog wel beter kunnen met de prioriteit van privacy in zorginstelling A. Ook moet het budget van de privacywerkgroep vooral gebruikt worden om medewerkers van te betalen en niet om campagnes op te zetten. : 'Het is volgens mij vooral budget voor de medewerkers'.

Er is een risico-inventarisatie gedaan
Er is een risico-inventarisatie gedaan bij zorginstelling A. Over het risico op een datalek zegt A: 'Je meldt het bijvoorbeeld niet, je komt toch in het nieuws of je neemt niet genoeg beveiligingsmaatregelen. Daar kun je vrij hoge boetes voor krijgen. Wij geven dat natuurlijk wel aan'.

Risico's van een beveiligingsissue zijn in beeld bij bestuur
A weet niet zo goed of de Raad van Bestuur zicht heeft op het risico van een datalek. A: 'Ik sta dan toch iets te ver van de Raad van Bestuur af om dat te weten hoe zij ernaar kijken, dat weet ik eigenlijk ook niet zo goed. Het belang wordt wel erkend, maar hoe ze er precies naar kijken dat durf ik niet te zeggen'.

Er is op basis van risico-inventarisatie een beleidsdocument informatiebeveiliging opgesteld
Zorginstelling A heeft een beleidsdocument informatiebeveiliging en heeft ook een checklist informatiebeveiliging. Dit is een checklist voor het personeel om te kijken of ze voldoende rekening houden met informatiebeveiliging.

Er wordt regelmatig gecommuniceerd over het informatiebeveiligingsbeleid
Zorginstelling A heeft elk jaar de dag van de patiëntveiligheid. Hier staan allemaal standjes die met patiëntveiligheid te maken hebben. Hier brengen ze bijvoorbeeld ook de datalekken weer onder de aandacht. A zegt hierover: 'Het is heel groot, een soort van dorp met straten daarbinnen en in de grote straat is het dan met allemaal kraampjes, dat wordt groots aangekondigd van tevoren: 'de dag van de patiëntveiligheid, kom allemaal kijken!''. Ook heeft zorginstelling A een bijeenkomst voor medewerkers. A zegt hierover: 'Vorig jaar hadden we iemand die ging vertellen over wat kan identiteitsfraude allemaal, wat kan ermee gebeuren? Hoe erg is dat? En iedereen schrikt zich dan rot natuurlijk. En we hebben er weer één in november dan hebben we een hacker die gaat laten zien hoe en wat we allemaal aan het lekken zijn. Om ook, ja de bewustwording vooral dus weer te stimuleren zeg maar'. Ook hebben een aantal trainees een belevingsonderzoek gedaan naar privacy. Zij liepen mee met het primaire proces van verpleegkundigen en vroegen hen waar ze aan denken bij privacy en wat voor dilemma's ze tegenkomen in hun werk. A geeft aan dat ze aan dit onderzoek ook wel wat ambassadeurs hebben overgehouden, mensen die echt wel enthousiast zijn. Er wordt dus op verschillende manieren aandacht besteed aan het informatiebeveiligingsbeleid van zorginstelling A.

Er wordt gewerkt aan het verhogen van beveiligingsbewustzijn in de organisatie
Om de bewustwording van mensen te vergroten heeft zorginstelling A onder andere de 'wat zou je doen' campagne opgezet. 'Wat zou jij doen' was een campagne voor datalekken. A: 'Bijvoorbeeld: er ligt een dossier op de balie, wat zou jij doen?'. Deze campagne was bedoeld om mensen te prikkelen, zodat ze erover na gingen denken. A: 'Bewustwording ook van goh wat gebeurt er nou en hoe kan je dat voorkomen? Om mensen weer aan het denken te zetten van goh het is inderdaad wel herkenbaar. Of oja hier kan ik nog wel wat beter over nadenken of beter op letten'. De campagne bestond uit briefjes met wat zou jij doen erop en als je het flapje omdraait dan zie je de situatie. Het antwoord op de vraag moet je zelf bedenken en kwam op een gegeven moment op het intranet te staan. De dag van de patiëntveiligheid die hierboven staat beschreven is ook een voorbeeld van een manier waarop het beveiligingsbewustzijn van zorginstelling A vergroot kan worden. Zorginstelling A is dus op verschillende manieren bezig met het verhogen van beveiligingsbewustzijn in de organisatie. Ook doet zorginstelling A bewustwordingscampagnes en helpt de checklist informatiebeveiliging en privacybescherming als geheugensteuntje tijdens het werk.

Er zijn duidelijke procedures aanwezig voor het behandelen van beveiligingsincidenten
Zorginstelling A heeft voor datalekken één werkproces ingericht voor alle medewerkers. Ze hadden al een ICT-hulplijn en hebben deze lijn ook ingezet voor datalekken. A zegt hierover: 'De ICT-medewerker die aan de telefoon zit die heeft van ons een vragenlijst gekregen van wat ze moeten uitvragen en daar vullen ze de antwoorden in en dat sturen ze naar ons toe. Wij doen de beoordeling en dat komt dan naar ons toe. Dan pakken wij het op. Wij doen de beoordeling of het ook bij de autoriteit persoonsgegevens gemeld moet worden bijvoorbeeld. En of er maatregelen genomen moeten worden om het in de toekomst weer te voorkomen'. A belt vaak ook nog even terug naar degene die gemeld heeft, omdat ze vaak nog wel wat extra informatie nodig heeft en ze informeert de melder ook vaak of ze het meld aan de Autoriteit Persoonsgegevens. Dan meldt A het ook aan de leidinggevende van de afdeling. Zorginstelling A heeft dus een duidelijk werkproces ingericht voor medewerkers. Er is duidelijk hoe je een datalek moet melden en waar. De uitleg van de procedure zou nog wat specifieker kunnen of kunnen worden uitgebreid met meer opties.

Er wordt regelmatig over deze procedures gecommuniceerd
A geeft aan: 'Dat hebben we gedaan met een brief, dat is dan van de Raad van Bestuur, dat is een brief die gaat de hele organisatie door. En we hebben een intranet daar heeft het opgestaan'. Ook heeft zorginstelling A een eigen intranetpagina voor privacy waar ze ook informatie op hebben staan. Hier staan ook vragen op, zoals wat is nu een datalek en wanneer moet je bellen. Zorginstelling A heeft ook een aantal flyers gemaakt en dingen opgehangen in de instelling. Verder heeft de privacycommissie ook presentaties gegeven. A: 'We zijn wel bij verpleegkundigen overleg geweest bijvoorbeeld. Ja, beetje wel echt van die zorgafdelingen. Ik weet niet precies meer welke allemaal. Vaak wel een beetje op verzoek ook hoor, zo van: nou we willen nog wel wat extra informatie. We hebben die brief gelezen maar we snappen het nog niet helemaal'. Naast de presentaties zijn ook de andere communicatie-uitingen zoals de campagne: 'wat zou jij doen' vanuit de privacywerkgroep verzorgd. Zorginstelling A heeft verder een checklist informatiebeveiliging en privacybescherming. Deze checklist hadden ze al voor informatiebeveiliging, maar die is uitgebreid met privacydingen en ook met de Meldplicht Datalekken. Hier staat bijvoorbeeld op waar je een datalek moet melden en dat je je computer moet uitloggen als je even naar het toilet gaat. Er wordt dus regelmatig gecommuniceerd over de procedures omtrent datalekken in zorginstelling A op verschillende manieren en op verschillende momenten.

De gekozen maatregelen worden regelmatig geëvalueerd
Er worden datalekrapporten gemaakt en deze gaan naar de Raad van Bestuur.

Het beleid wordt na evaluatie indien nodig aangepast

7.2 Analyse zorginstelling B

Actieve betrokkenheid van het bestuur
Als het nodig is worden voorvallen besproken met de Raad van Bestuur bij zorginstelling B. B heeft met beide leden van de Raad van Bestuur maandelijks contact, maar dit komt ook omdat hij een gedeelde functie heeft en ook risicomanager is. B zegt: 'Wij doen een voorstel en natuurlijk kijken zij daar nog wel overheen van zijn we het daar helemaal mee eens'. Als er een melding wordt gedaan van een datalek of een mogelijk datalek dan gaat dit altijd eerst langs de Raad van Bestuur voordat bijvoorbeeld de Autoriteit Persoonsgegevens wordt

ingelicht. De Raad van Bestuur kan uiteindelijk beslissen of zij de AP inlichten. De verantwoordelijkheid ligt dus bij de Raad van Bestuur. B geeft aan dat de Raad van Bestuur ook hoofdelijk aansprakelijk is op het moment dat het fout gaat, dus hij vindt het heel logisch dat zij degene zijn die daar een eindoordeel over vellen. De Raad van Bestuur is dus actief betrokken bij het afhandelen van meldingen en er is maandelijks contact met de Raad van Bestuur.

Prioriteit van privacy in organisatie
De Raad van Bestuur geeft niet aan of er aandacht moet worden gegeven aan privacy. B zegt: 'Nee, eigenlijk komt dat nauwelijks voor. Dat gaat andersom. Wij komen met voorstellen van hier zouden we aandacht aan moeten besteden en dat adviseer je dan en dan wordt dat door hen besloten. Zo gaat dat in de praktijk'. B besteedt ongeveer een dagdeel per week aan zijn functie als functionaris gegevensbescherming. Fulltime zou voor een instelling als zorginstelling B veel te duur zijn. De Raad van Bestuur geeft niet aan dat er aandacht moet worden gegeven aan privacy en de functie van FG moet niet teveel geld kosten. Er lijkt dus geen prioriteit voor privacy te zijn in zorginstelling B.

Er is een risico-inventarisatie gedaan
Er is een risico-inventarisatie gedaan bij zorginstelling B. B geeft aan dat de risico's voor zorginstelling B niet anders zijn dan voor andere zorginstellingen. Er is heel veel aandacht voor de boetes die je kunt krijgen als je een datalek niet meldt. B denkt zelf dat de risico's veel groter zijn op het vlak van imagoschade en dat soort dingen. Dat zijn de belangrijkste risico's bij privacyschending volgens B.

Risico's van een beveiligingsissue zijn in beeld bij bestuur
B geeft aan dat er heel veel aandacht is voor de boetes die je kunt krijgen. Er is dus wel aandacht voor de boetes die je kunt krijgen, maar geen aandacht voor andere risico's zoals reputatieschade of verlies van patiëntvertrouwen.

Er is op basis van risico-inventarisatie een beleidsdocument informatiebeveiliging opgesteld
Het beleid wordt opgesteld door de mensen onder de Raad van Bestuur. Zorginstelling B heeft een privacybeleid en heeft procedures opgesteld rondom datalekken. Ook heeft zorginstelling B een loginbeleid en een procedure voor wat je wel en niet op lokale media mag opslaan. Het is bijvoorbeeld zo dat usb-uitgangen in principe niet werken, alleen op aanvraag en op argumentatie worden die open gezet. Als mensen het ziekenhuissysteem in willen dan moeten ze hun account openen en dat kan zorginstelling B vanaf afstand stoppen, maar wat mensen lokaal hebben opgeslagen daar kan B niet bij. Eén keer in de maand leest B ook logins uit van het EPD en kijkt B wie toegang heeft gekregen tot welk dossier en of deze toegang terecht is geweest. Als mensen onrechtmatig toegang hebben gekregen dan worden ze gemaild en als er sprake is van een privacyschending dan krijgen medewerkers ook echt een gesprek met B en hun leidinggevende.

Er wordt regelmatig gecommuniceerd over het informatiebeveiligingsbeleid
B geeft aan dat je communicatie moet opsplitsen. Je doet algemene communicatie zoals in een weekblaadje. Daar staat af en toe wat in. En je kunt via de lijn communiceren, omdat je bepaalde groepen beter wilt bereiken. B is vorig jaar begonnen met risicomanagement en geeft aan dat je jezelf dan ook moet presenteren en duidelijk moet maken waarover het gaat als je het hebt over risico's. Informatiebeveiliging komt dan ook aan bod. B heeft presentaties gegeven in iedere sector van het ziekenhuis. Wat B ook graag zou willen is dat er casussen besproken worden op afdelingen, maar dat staat nog op zijn lijstje.
Met artsen wordt gecommuniceerd via het stafbestuur. Zij hebben stafoverleg één keer in de zoveel tijd. Ook kun je ze bereiken via een mailing.

Er wordt gewerkt aan het verhogen van beveiligingsbewustzijn in de organisatie
Er komt steeds meer bewustzijn van medewerkers, maar medewerkers bereiken is lastig. 'Je hebt bij iedere communicatie een zender en een ontvanger en dat is lastig, want die ontvanger daar heb je in feite geen invloed op. Als je iets niet wil horen, dan hoor je niks'. Wat je ziet gebeuren bij het uitlezen van logins en checken wie in welk dossier heeft gezeten is dat mensen onderling gaan praten over dat ze een mail krijgen en verantwoording af moeten leggen. B krijgt nu zelfs soms mailtjes van mensen die zeggen met welke reden ze in een dossier zijn geweest. B geeft aan dat dat natuurlijk is wat je wilt: 'Je wilt dat mensen erover na gaan denken van moet ik hier wel in?'. Deze methode werkt volgens B. 'Dit werkt beter dan één keer in de week in

zo'n blaadje wat zetten, want dat leest toch echt niet iedereen hoor'. Mensen denken dus wel over beveiliging na, maar zij worden niet actief door zorginstelling B op weg geholpen naar een hoger beveiligingsbewustzijn.

Er zijn duidelijke procedures aanwezig voor het behandelen van beveiligingsincidenten
In de VIM-applicatie (Veilig Incidenten Melden) is een categorie informatiebeveiliging gemaakt. Als medewerkers daar een melding maken, dan krijgt B daar samen met de twee andere leden van de informatiebeveiligingscommissie een mail van. Vervolgens gaat B aan de slag om te kijken wat er precies gebeurd is en of het gemeld moet worden aan de autoriteit persoonsgegevens. Ook kijkt B hoe het lek gedicht moet worden. De medewerker krijgt vaak een terugrapportage. B zit in een team van drie dus er is altijd iemand aanwezig, dat maakt dat de 72 uurs deadline haalbaar is. Naast de VIM-applicatie kan er ook gebeld worden naar B, zijn nummer staat op internet. Vanuit extern kun je niet bij de VIM-applicatie, maar je kunt wel contact opnemen met B. Als je op privacy zoekt, dan kom je bij B terecht.
Als er een informatiebeveiligingsincident is dan is er een commissie die dat onderzoekt. B is degene die dat praktisch onderzoekt en maakt dan een rapport. Die stuurt B naar de andere twee leden. Zij bespreken dit rapport eerst samen en dan gaat het rapport naar de Raad van Bestuur. Als het een lastig te beoordelen incident betreft dan kan ook nog de jurist of de autorisatiecommissie worden ingeschakeld om te helpen. Zorginstelling B heeft duidelijke procedures over het behandelen van beveiligingsincidenten.

Er wordt regelmatig over deze procedures gecommuniceerd
De communicatie over de procedures is geheel algemeen gegaan langs twee sporen: het algemene nieuwsblaadje van het ziekenhuis en via het MT naar de lijn, omdat een datalek in feite overal in een organisatie kan voorkomen. Er zijn geen flyers gemaakt. Er is aandacht aan besteed in de nieuwsbrief en daarin is verwezen naar het intranet. Op het intranet staan ook voorbeelden van waar je aan moet denken bij een datalek. B geeft aan dat ze gecommuniceerd hebben over de Wet Meldplicht Datalekken. Ze hebben gecommuniceerd dat de wet er is en hoe medewerkers datalekken moeten melden. Dat gaat overigens op dezelfde manier als ieder ander veiligheidsincident, maar is wel opnieuw gecommuniceerd. Medewerkers horen te weten hoe ze incidenten moeten melden, aangezien andere incidenten op dezelfde manier gemeld moeten worden als datalekincidenten. Zorginstelling B heeft dus over de procedures datalekken op verschillende manieren gecommuniceerd. Echter is de vraag of er nog steeds actief over deze procedures gecommuniceerd wordt, aangezien zorginstelling B in de verleden tijd spreekt.

De gekozen maatregelen worden regelmatig geëvalueerd
B zou graag willen dat casussen worden besproken op afdelingen, maar dit is op dit moment nog niet zo.

Het beleid wordt na evaluatie indien nodig aangepast

7.3 Analyse zorginstelling C

Actieve betrokkenheid van het bestuur
Op dit moment is de functie van functionaris voor de gegevensbescherming direct onder de Raad van Bestuur belegd. Vanuit het MT was er behoefte om de belangrijkste speerpunten rondom informatiebeveiliging op een A4tje te zetten, maar dat waren inmiddels drie A4tjes geworden, dus toen werd aangegeven dat C misschien eens met communicatie moest gaan praten.
Een incident wordt teruggekoppeld aan de bestuurder met C's advies om het wel of niet te melden bij de AP. De Raad van Bestuur bepaalt uiteindelijk om te gaan melden, dus die zijn volgens C heel dicht betrokken. C: 'Ja, zij zijn eindverantwoordelijk, dus ik wil wel graag dat horen en dat op schrift hebben dat hij akkoord is met de melding, maar uiteindelijk adviseer ik wel dringend om dat te melden of om het niet te melden'.
De Raad van Bestuur heeft het privacythema in beeld via de stuurgroep. De voorzitter van de Raad van Bestuur zit namelijk in de stuurgroep. Meldingen gaan ook via de Raad van bestuur. De Raad van Bestuur van zorginstelling C is dus zeer actief betrokken bij het privacythema.

Prioriteit van privacy in organisatie
Er is een stuurgroep informatiebeveiliging en daar zit de bestuurder ook bij, de informatiemanager en C. Ook is er een klankbordgroep die elk kwartaal bij elkaar komt. De stuurgroep komt maandelijks bij elkaar. Daarnaast heeft zorginstelling C maandelijks MT en daar staat dit punt ook op de agenda. C geeft aan dat het in die zin dus wel gebord is overal, maar dat ze op dit moment wel in een periode zitten waar andere zaken ook hoge

prioriteit hebben en dan merk je toch dat het bij mensen overkomt als 'oh heb je dat gezeur weer'. C vindt dat privacy een hoge prioriteit heeft bij heel veel mensen, maar ze denkt dat het bij medewerkers die echt zorg willen verlenen nog niet zo erg meespeelt.
Communicatie is bij zorginstelling C wat meer ondersteunend. C: 'Het is niet echt zo dat zij het voortouw nemen van we gaan een campagne opstarten. En dat is ook weer een beetje omdat dan die prioriteiten weer anders liggen.' Deze prioriteiten liggen meer op extern voornamelijk bij uitvoerende diensten zoals folders up-to-date houden en foto's.
Er is in zorginstelling C op bestuursniveau zeker prioriteit voor privacy. In de rest van de organisatie denkt C dat dit nog wat minder is.

Er is een risico-inventarisatie gedaan
Ja, er is een risico-inventarisatie gedaan. C geeft aan: 'Op ICT-gebied word ik echt ondersteund door de informatiemanager en hij is ook vorig jaar al betrokken geweest bij onder andere de risico-inventarisatie'.
C is niet zozeer bang voor een datalek, dat kan iedereen overkomen. C is ervan overtuigd dat als je maar transparant en helder bent en duidelijk bent in je communicatie naar buiten dat je dan niet zo'n heel groot risico loopt. Wel als je het gaat achterhouden en gaat verzwijgen.

Risico's van een beveiligingsissue zijn in beeld bij bestuur
C geeft aan dat die risico's wel in beeld zijn bij de Raad van Bestuur. De Raad van Bestuur is vorig jaar betrokken geweest bij de werkgroep die een risico-inventarisatie heeft gedaan. C was daar toen nog niet bij betrokken. C geeft aan dat de risico's wel in beeld zijn bij de Raad van Bestuur, maar er worden geen voorbeelden genoemd van risico's.

Er is op basis van risico-inventarisatie een beleidsdocument informatiebeveiliging opgesteld
C geeft aan dat er geen security of privacybeleid was, dus dat ze daar vorig jaar mee aan de gang zijn gegaan. De informatiemanager heeft daar het voortouw in genomen. Hij is ook tevens MT-lid. C heeft op basis daarvan een informatiebeveiligingsplan geschreven en een plan van aanpak Meldplicht Datalekken, dus met die drie notities is er één grote notitie gemaakt en die is begin van dit jaar ook in het MT vastgesteld en die wordt nu geïmplementeerd in de organisatie verder. Er zijn nog geen maatregelen bij het niet naleven van de regels, omdat daar nog geen duidelijk beleid over is. C wil daar wel sancties aan gaan ophangen.
C heeft de uitslagen van de risico-inventarisatie overgenomen en toen de risico's uitgezet bij de probleemeigenaren. De probleemeigenaren moesten vervolgens aan de hand van die opdracht een plan van aanpak schrijven en die wordt dan weer teruggekoppeld in de stuurgroep en gaat weer mee in het MT.
C merkte dat er ook behoefte was aan algemene gedragscodes. Zorginstelling C heeft heel veel losse dingen: ICT-regels, huisregels, gedragsregels, maar eigenlijk mist een algemeen beeld.
Er is toen een inventarisatie gemaakt in vier categorieën: papier, techniek, applicaties en gedrag. Hieronder werden de verschillende risico's beschreven en vervolgens was de opdracht om aan de hand van die risico's een plan van aanpak te maken.
Bij zorginstelling C is het beleid om niet te werken met USB-sticks, je kan namelijk overal toegang krijgen tot het systeem door in te loggen. Dit is opgenomen in de ondernemingsovereenkomst: geen gebruik maken van USB-sticks.

Er wordt regelmatig gecommuniceerd over het informatiebeveiligingsbeleid
Het informatiebeveiligingsbeleid en het privacyreglement zijn gepubliceerd op intranet. C: 'Ja dat kunnen mensen lezen op intranet, maar dat is niet actief. Ja, het staat daar'. C wil het daarom onderdeel laten uitmaken van het functioneringsgesprek, een agendapunt, zodat het daar ook besproken wordt. Er is binnenkort een privacy training. Deze wordt gegeven door een advocatenkantoor. Ook maakt zorginstelling C gebruik van nieuwsbrieven, die worden maandelijks verstuurt door C. Binnenkort gaat er een enquête uit gebaseerd op de NEN-7510 als een soort nulmeting van hoe het nu leeft bij de mensen. Die wordt dan zowel op topniveau als bij de mensen op de werkvloer uitgezet en dan wil zorginstelling C hem over een half jaar weer gaan herhalen om te kijken of het veranderd is en waar mensen behoefte aan hebben. Ook hoe zij graag informatie aangedragen zouden krijgen. C geeft aan dat communicatie wel altijd als een zwak punt naar boven komt bij de medewerkersmonitor.

De communicatie gaat in eerste instantie vanuit de top. C: 'Het MT heeft die stukken vastgesteld, dan gaan die stukken via het betreffende MT-lid verder naar de divisie naar de leidinggevenden en de leidinggevenden die nemen dat dan weer mee in hun overleggen met de teams.
Alle groepen worden op dit moment nog op dezelfde wijze benaderd. Wat lastig is, is dat niet alle groepen toegang hebben tot het intranet, omdat niet alle medewerkers een eigen account hebben. Ook hebben zij geen werkoverleggen dus dat is een lastige groep om te bereiken.
Zorginstelling C heeft ook aangehaakt bij Alert Online. Ze heeft meegedaan met de quiz die online beschikbaar stond en ze heeft iedere dag bij het inloggen een leus of een korte tekst over informatieveiligheid geplaatst, telkens een ander onderwerp met een plaatje erbij.
Zorginstelling C geeft aan dat het informatiebeveiligingsbeleid gepubliceerd staat op intranet, maar dat dat niet actief is en dat er wel nieuwsbrieven verstuurd worden en via het MT gecommuniceerd wordt over informatiebeveiliging. Er wordt dus wel regelmatig gecommuniceerd (maandelijkse nieuwsbrief) over informatiebeveiliging.

Er wordt gewerkt aan het verhogen van beveiligingsbewustzijn in de organisatie
Er wordt binnenkort een training privacy gegeven. Ook is er een extern communicatieadviseur aangetrokken. Zij had verschillende ideeën één daarvan was om een digitaal poppetje te creëren die af en toe over je scherm komt met een kreet. Dat is wel iets wat mensen bijblijft en dat poppetje is dan gekoppeld aan informatiebeveiliging. Er wordt dus wel gewerkt aan het verhogen van beveiligingsbewustzijn.
C geeft aan: 'In het begin was er echt radiostilte. Je merkt wel dat er gaandeweg meer over gecommuniceerd wordt en dat er steeds meer mailtjes bij mij komen'.
C geeft aan dat het wel lastig is om medewerkers te motiveren om te gaan melden de MIC-melding (Melding Incident Cliëntenzorg) of MIM-melding (Melding Incidenten Medewerker) wordt bij C ook nauwelijks gedaan.

Er zijn duidelijke procedures aanwezig voor het behandelen van beveiligingsincidenten
Zorginstelling C heeft een interne meldingsprocedure voor datalekken. Op het intranet staat een intern meldingsformulier. C: 'Dat wordt nog niet zo vaak gebruikt. Het merendeel gaat toch via de mail gegevensbescherming'. De medewerkers worden ook meegenomen in het proces als zij een melding doen. C: 'Er volgt altijd een terugkoppeling hoe we ermee om zijn gegaan'.
Zorginstelling C heeft geen algemeen calamiteiten plan. C: 'We hebben wel een calamiteitendienst voor het weekend, maar ja als er een echte calamiteit is wat moet er dan gebeuren en hoe gaan we evacueren of wat dan ook, dat hebben we dus allemaal niet'. Er is dus wel een procedure voor datalekken, maar deze wordt nog niet zo vaak gebruikt en zorginstelling C heeft ook geen algemeen calamiteitenplan.

Er wordt regelmatig over deze procedures gecommuniceerd
Er is via een nieuwsbrief over de Wet Meldplicht Datalekken gecommuniceerd. Ook staat er een stuk op intranet waar het plan van aanpak beschreven staat. C heeft ook een stukje geschreven op het intranet dat de wet is ingegaan en er was een informatiebijeenkomst. C heeft net een medewerkersbijeenkomsten achter de rug, waarin dit onderwerp ook werd aangestipt. Deze bijeenkomsten is zorginstelling C gestart omdat de werkoverleggen eigenlijk wat geskipt werden vanwege reistijd en productiviteit. Bij de medewerkersbijeenkomsten worden actuele zaken besproken. De opkomst is heel wisselend. Voor de privacyworkshop wil C aan de hand van stellingen en aan de hand van praktijkcasussen een interactieve sessie hebben. Dus er is aan medewerkers gevraagd waar zij tegen aan lopen en daar komen wel reacties op binnen. De privacyworkshop is voor de top: het MT, de leidinggevenden, de afdeling finance en control en de ICT-afdeling. Maar de stellingen en praktijkcasussen kun je wel meenemen in je werkoverleg.
Er wordt dus op verschillende manieren gecommuniceerd over de procedures.

De gekozen maatregelen worden regelmatig geëvalueerd
C's eerste antwoord is nee. Als iets vaker voorkomt dan nemen ze het wel mee. Issues waarvan C denkt dat ze daar wat mee moeten in de organisatie koppelt C terug aan de stuurgroep en dan geeft C daar advies over en dan bepaalt de bestuurder of hij het advies wel of niet overneemt, dus dat komt wel iedere keer terug in de cyclus.
Er is in zorginstelling C bijvoorbeeld gekeken hoe het komt dat er geen meldingen worden gedaan (ook geen MIC en MIM meldingen). Er is gekeken hoe dit anders kan en dan is daar weer ander beleid op gekomen, maar het verandert nog niet.

Het beleid wordt na evaluatie indien nodig aangepast
Ja, zie voorbeeld hierboven.

7.4 Analyse zorginstelling D

Actieve betrokkenheid van het bestuur
D valt vrij direct onder de Raad van Bestuur. Formeel zit daar nog een directiesecretaris tussen voor de arbeidsvoorwaardelijke zaken, maar D zit niet bij een organisatieonderdeel. Zorginstelling D heeft een afdeling informatiemanagement en met dat hoofd zet D nu het beleid op. D: 'We hebben inmiddels maandelijks overleg met één van de directeuren over nou ja wat is nu de stand van zaken en daar zit natuurlijk de Raad van Toezicht achter die willen ook weten wat de stand van zaken is. En dat is wel dat merk je bij zo'n Wet Datalekken er wordt met hoge boetes gedreigd en dan ontstaat een soort schrikeffect ook bij bestuurders zo van hebben we het wel op orde'.
Het bestuur is dankzij de maandelijkse overleggen actief betrokken bij het informatiebeveiligingsbeleid.

Prioriteit van privacy in organisatie
D valt bijna van zijn stoel als hij soms hoort hoe iemand vanuit hoger management nog fouten maakt bij het naleven van basisregels. D: 'Er staat duidelijk opgeschreven dat je geen persoonsgegevens naar privéadressen mag sturen dat alles binnen ons netwerk moet blijven. En ik hoorde gisteren toevallig weer dat vanuit hoger management nog daar onbekendheid mee was dat er tegen een medewerker werd gezegd, nou dan stuur je het toch even naar je huismailadres'.
D geeft aan dat hij meer moeite heeft gehad het bestuur gerust te stellen dan het bestuur bang te maken voor een boete mede door de grote aandacht in de commerciële hoek.
Volgens D heeft privacy in de instelling een hoge prioriteit. D: 'Wij hebben zo'n 20.000 patiënten per jaar en als je dan kijkt naar het aantal incidenten die in ieder geval bij mij bekend worden dan is dat niet veel. Het leidt niet heel vaak tot ernstige incidenten waarvan je echt denkt nou dit is heel erg'.
D geeft aan dat er op bestuurlijk niveau heel veel aandacht voor is geweest toen de Wet Meldplicht Datalekken kwam. D heeft heel veel vragen gekregen zoals: waar staan we en wat zijn onze risico's? Maar in de organisatie zelf is er nog niet heel veel aandacht voor geweest.
Het bestuur had wel angst voor de boete en er is veel aandacht geweest op bestuurlijk niveau voor de Meldplicht Datalekken. Echter komt het nog wel eens voor dat mensen van hoger management zich niet aan de regels houden. Privacy heeft dus wel prioriteit in zorginstelling D, maar het bestuur zou nog wel wat beter kunnen tonen dat het prioriteit heeft.

Er is een risico-inventarisatie gedaan
Ongeveer een jaar geleden is de functie van FG ingesteld en toen heeft D aangegeven dat er een nulmeting moest komen. Een extern bureau heeft toen een privacy impact assessment laten doen.
Over de risico's voor de instelling zegt D: 'Ik denk dat het grootste risico als instelling de imagoschade is die je op kunt lopen en eventueel de financiële schade. Het zou natuurlijk plat gezegd heel gênant zijn als patiëntgegevens op straat komen te liggen'.
De grootste kwetsbaarheid is de menselijke factor. Technisch is het wel dichtgespijkerd, zelfs als je er het beleidsdocument op na slaat dan denk je nou dat ziet er allemaal wel netjes uit, maar mensen moeten zich er ook naar gedragen, dus dat betekent dat mensen moeten weten wat ze wel en niet mogen en dan ook nog doen'.

Risico's van een beveiligingsissue zijn in beeld bij bestuur
Er is op bestuurlijk niveau veel aandacht geweest voor de Wet Meldplicht Datalekken. Het bestuur wilde graag weten waar de organisatie staat en wat de risico's zijn. Ook willen ze maandelijks op de hoogte blijven en zijn ze geschrokken van de boete die je kunt krijgen. De risico op een boete is dus in beeld bij het bestuur en het bestuur blijft graag betrokken bij de risico-inventarisatie.

Er is op basis van risico-inventarisatie een beleidsdocument informatiebeveiliging opgesteld
In technische zin heeft zorginstelling D volgens D het wel redelijk goed voor elkaar, omdat er wel autorisatieregels zijn, maar de awareness, het toezicht en het sanctiebeleid daar moet zorginstelling D nog wel mee aan de slag.

Er wordt sinds de nieuwe wet meer gekeken naar het integrale beleid. D: 'We hebben wel allerlei documenten over privacy, beroepsgeheim, over wat je wel en niet mag en moet, maar ja het is natuurlijk zo breed, het zit natuurlijk overal in. Dus je wilt ook het totaalplaatje'.
Zorginstelling D heeft een elektronisch documentensysteem en daar staat alle informatie daar staan alle beleidsafspraken en regels in. D geeft aan dat dat een vrij statisch iets is en dat mensen al moeite moeten nemen om erin te gaan kijken.
Je kunt overal inloggen op het systeem van zorginstelling D. En er is ook een protocol geschreven voor het anonimiseren van gegevens: 'Hoe doe je dat en wanneer vinden wij dat het geen persoonsgegevens meer zijn'.

Er wordt regelmatig gecommuniceerd over het informatiebeveiligingsbeleid
Er is nu één gesprek geweest met communicatie om te kijken hoe ze een voorlichtingscampagne op kunnen zetten en ook of de focus meer zal liggen op datalekken of op de algemene privacy. G zegt hierover: 'Dat zal beiden zijn. Het zal een campagne worden met verschillende aspecten, waarin we het principe van datalekken en het melden ervan op een redelijk eenvoudige manier naar voren willen brengen door toch heel kort uit te leggen van wat is het en wat doe je? Bij wie meld je dat? En wat gebeurt er dan mee? Maar het hele privacyaspect dat zal doorlopende informatie moeten zijn'.
Mogelijke communicatievormen voor de voorlichting zijn het intranet en een intern magazine dat met enige regelmaat uitkomt. D geeft aan: 'En ja verder kan ik wel gaan fantaseren maar we hebben het nog niet uitgewerkt'.
Op dit moment wordt er nog niet heel veel anders gedaan dan gecommuniceerd via het digitale documentatiesysteem. Ook wordt D wel eens uitgenodigd op een afdeling om iets erover te vertellen. Dan gaat het meestal vanuit de regels van het beroepsgeheim, wat mogen we nou wel delen en wat niet. Het meer push zoals posters en nieuwsberichten moet nog komen. Er wordt dus niet regelmatig gecommuniceerd over het informatiebeveiligingsbeleid.

Er wordt gewerkt aan het verhogen van beveiligingsbewustzijn in de organisatie
Als er een incident geweest is dan is er enorme awareness op de betreffende afdeling D: 'Alleen hoe draag je dat dan over aan de rest van de organisatie en dat is moeilijk. En ik verwijt ons ook wel dat we niet echt een hele goede lerende organisatie zijn. Ja dat is niet bewust, maar om nou te zeggen van 'ja goh let erop want daar en daar is dit misgegaan'. Dat is toch een beetje als je vuile was buiten hangen'.
Er wordt in zorginstelling D nog niet actief gewerkt aan het verhogen van beveiligingsbewustzijn. Er is pas één gesprek geweest met communicatie om te kijken naar een campagne.

Er zijn duidelijke procedures aanwezig voor het behandelen van beveiligingsincidenten
Er staat nu in het privacydocument dat je een datalek moet melden bij de functionaris gegevensbescherming, maar D wil nog een campagne en een apart schemaatje om alles te versimpelen.
Op dit moment kunnen ze op twee manieren melden. Zorginstelling D heeft een incident-meldsysteem of je kunt het melden bij je leidinggevende en dat je leidinggevende het bij mij meldt. D probeert vervolgens vooral te onderzoeken hoe zorginstelling D kan voorkomen dat het weer gebeurt.
Er zijn dus wel manieren van melden geïntroduceerd, maar er worden geen details gegeven over deze manieren. Er moet hierover ook nog een campagne komen voor medewerkers.

Er wordt regelmatig over deze procedures gecommuniceerd
Er zijn in het verleden al campagnes geweest op het incident-meldsysteem en die werkten. Er hoeft hier geen aparte training meer voor gegeven worden. Op dit moment is zorginstelling D nog bezig met het opstellen van een communicatieplan.
Volgens D weten medewerkers hoe het incident-meldsysteem werkt en hoeft hier niet opnieuw in getraind te worden. Er is nog geen communicatie over de procedures.

De gekozen maatregelen worden regelmatig geëvalueerd
Er worden geen casussen besproken in zorginstelling D: 'Nee, als er een groot onderzoek is geweest omdat er een calamiteit is geweest. Dat komt niet op intranet van goh dit zijn de bevindingen geweest en dit zijn de verbetermaatregelen en hé jongens wil iedereen daar even op letten, terwijl dat in mijn ogen wel goed zou zijn om dat wel te doen. Je moet natuurlijk altijd oppassen dat je niet ook de privacy van de medewerkers schendt,

maar ja met een beetje goede wil'. Hierboven geeft D ook aan dat zorginstelling D niet echt een goede lerende organisatie is.

Het beleid wordt na evaluatie indien nodig aangepast
Een voorbeeld van het aanpassen van beleid na evaluatie is het SPSS-voorbeeld. Eerst had zorginstelling D allemaal losse versies van SPSS maar die stonden op laptops die mensen meenamen en dat vond zorginstelling D wel een risico. Dat heeft zorginstelling D verbeterd door een netwerkversie aan te schaffen. Nu hoeven onderzoekers niks extern meer te doen, want ze kunnen thuis ook inloggen op het systeem.

7.5 Analyse zorginstelling E

Actieve betrokkenheid van het bestuur
De bestuursstaf gaf aan dat het geen losstaand initiatief moest zijn, maar dat het gedragen moet worden vanuit het bestuur. Alleen dan kun je ervoor zorgen dat je voldoende maatregelen kunt treffen als organisatie. E: 'Het is niet alleen een technisch stuk, maar ook een organisatorisch stuk en daar heb je gewoon de support en het mandaat van het bestuur voor nodig. Dus het bestuur staat daar helemaal achter. Daar hebben we ook mee aan tafel gezeten en uitgelegd wat we willen'.
Het plan van aanpak is goedgekeurd door het bestuur. E: 'Onderdeel daarvan is dat de mensen van de bestuursstaf waarmee ik gesproken heb die zijn nu lid geworden van het zogenaamde p-team, het privacyteam. En zij zijn degene die de afhandeling doen van de meldingen die er komen, maar ook die zich bezighouden met allerhande zaken die te maken hebben met privacy'.
Het bestuur zelf zal niks doen met de meldingen, de bestuursstaf wel. Er vindt niet perse overleg plaats met het bestuur voor er een melding wordt gedaan.
Het bestuur van zorginstelling E staat achter het beleid en E geeft aan dat er mandaat van het bestuur nodig is voor het goed doorvoeren van beleid, dus dat er wel aan tafel is gezeten met de Raad van Bestuur. De bestuursstaf zit bovendien in een privacyteam om meldingen af te handelen. Het bestuur is dus actief betrokken bij informatiebeveiliging en privacybescherming.

Prioriteit van privacy in organisatie
E heeft de Wet Meldplicht Datalekken onder de aandacht gebracht bij de bestuursstaf en toen werd vanuit de bestuursstaf de wens uitgesproken of E niet als functionaris gegevensbescherming aan de slag kon gaan. E is functionaris gegevensbescherming sinds februari 2016. Er is een plan van aanpak voor de komende twee jaar en er is een privacyteam waarin ook het bestuur een rol speelt. Er is dus wel prioriteit voor privacy in zorginstelling E.

Er is een risico-inventarisatie gedaan
E is bezig met het uitvoeren van een privacyhuishouding. Daarnaast doet zorginstelling E een risicoanalyse op elk systeem en daarin zit bijvoorbeeld: welke maatregelen hebben we? Wat is de aard van de gegevens? Wat is het risico dat daar een datalek in gaat ontstaan? En aan de hand daarvan heeft zorginstelling E een lijst met huidige maatregelen en ook een rationele afweging van waarom je dan iets wel of niet kiest.
Over de risico's van een datalek zegt E: 'Als de behandelgegevens op straat komen te liggen, dan vertrouwt een cliënt ons niet meer en dan heeft die cliënt mogelijk echt wel grote persoonlijke schade. Dus dat is een ding, dat is voor ons zeer zwaarwegend. Qua instelling hebben we reputatieschade. We willen niet in het nieuws komen dat er dossiers van cliënten op straat liggen. Een ander gevolg is de boete'.

Risico's van een beveiligingsissue zijn in beeld bij bestuur
E geeft aan dat de risico's in beeld zijn bij het bestuur. Het kostte E twee zinnen in een mailtje om aan te geven dat de bestuurder aansprakelijk is en als er een boete komt de bestuurder degene is die moet gaan betalen. Het risico op een boete is dus in beeld bij het bestuur. Andere risico's worden niet genoemd.

Er is op basis van risico-inventarisatie een beleidsdocument informatiebeveiliging opgesteld
E heeft een plan van aanpak geschreven voor een periode van twee jaar waarin E aangeeft hoe ze gaan werken aan het organiseren van gegevensbescherming binnen zorginstelling E. E: 'Wat we nu aan het doen zijn is het inventariseren en het verzinnen van zinvolle stappen en dan in fase 2 gaan we dat expliciet uitvoeren en

uitrollen en daar zijn we natuurlijk al mee bezig maar daar is fase 2 eigenlijk echt voor. In fase 3 dat heet reflectie en borgen dus dan gaan we het evalueren.

Er wordt regelmatig gecommuniceerd over het informatiebeveiligingsbeleid
Zorginstelling E heeft ervoor gekozen eerst de datalekken als thema aan te pakken binnen het informatiebeveiligingsbeleid. De communicatieafdeling wordt wel betrokken bij het opstellen van een communicatieplan. Dit plan moet nog in uitvoering gebracht worden maar bestaat onder andere uit regelmatig terugkerende korte presentaties in teamoverleggen, privacy standaard op de agenda, het maken en verspreiden van flyers en regelmatige berichtgeving op intranet. Ook heeft E het plan om op de screensaver van koffieautomaten een privacypoppetje te doen.
E is ook op de hoogte van de 'ZEKER' campagne van de NVZ. Ze hebben het materiaal van deze campagne al klaarliggen en willen dit gaan ophangen. Er hebben ook 40 medewerkers mee gedaan aan de test die hoorde bij de 'ZEKER' campagne.
De communicatie verschilt niet van groep tot groep, omdat er een standaard werkomgeving is. E: 'Iedereen komt op dezelfde manier op het systeem en krijgt daardoor dus eigenlijk toegang tot dezelfde communicatie'.
Er zijn bij zorginstelling E dus wel plannen om over het informatiebeveiliging en privacybescherming te communiceren, maar dit moet allemaal nog tot uitvoering worden gebracht.

Er wordt gewerkt aan het verhogen van beveiligingsbewustzijn in de organisatie
E geeft aan dat communicatie heel belangrijk is in hoe je hiermee omgaat als organisatie. E: De manier waarop we dat doen is dus door veel de hort op te gaan, door veel het onderwerp te bespreken, door bewustwording proberen te kweken door bijvoorbeeld die stellingen en dat onder de aandacht te brengen, mensen snel terugkoppeling te geven'. Ook door bijvoorbeeld bewustzijn te creëren bij de helpdesk, want zij hoeven geen cliëntendossiers te zien om een probleem op te lossen. Op dit moment wordt er bij zorginstelling E nog passief gewerkt aan het verhogen ven beveiligingsbewustzijn. Bovenstaande manieren van communicatie staan nog in het beginstadium. Ze moeten nog worden ingepland.

Er zijn duidelijke procedures aanwezig voor het behandelen van beveiligingsincidenten
In het datalekprotocol staat wat je moet doen bij een datalek. Je kunt dan melden via de mail, je leidinggevende informeren of een veiligheidsmelding doen. Vervolgens gaat het privacyteam aan de slag en stelt eventueel vragen aan de lijnorganisatie. Na een melding wordt afhankelijk van de aard van de melding teruggekoppeld aan de medewerker.
Er worden ook veiligheidsrondes gedaan door de kwaliteitsadviseur.
Issues komen in de jaarrapportage en in de kwartaalrapportage naar het bestuur en daarin worden ook adviezen gegeven om in de toekomst dit soort issues te voorkomen.
E: 'Er wordt gemeld met een redelijke hoeveelheid maar ik denk dat dat meer zou mogen zijn en voorheen ja kijk de geheimhoudingsplicht, de medische geheimhoudingsplicht zit bij veel mensen goed tussen de oren dus er zit al een groot gevoel van awareness van cliëntgegevens mag je niet zomaar delen. Ik kan nog niet echt zien dat de bewustwording hoger is geworden ofzo'.
Er is een datalekprotocol opgesteld en er is een privacyteam.

Er wordt regelmatig over deze procedures gecommuniceerd
In het datalekprotocol wordt uitgelegd wat een datalek is, wat voorbeelden zijn en wordt een beslisboom gegeven van wanneer gemeld moet worden. Ook wordt aangegeven wie waarover gaat in de organisatie. Het protocol Meldplicht Datalekken is gecommuniceerd aan de hele organisatie. Dat brengt zorginstelling E regelmatig onder de aandacht. E: 'Ja, ze kunnen via intranet zoeken, ze kunnen het nieuwsbladbericht erbij pakken als ze die nog weten te vinden, ze kunnen via het kwaliteitssysteem en daar wordt iedereen in getraind, iedere nieuwe medewerker krijgt een training en dan kunnen ze het via het kwaliteitssysteem opzoeken. En op het moment dat die intranetpagina er is, dan staan daar ook allerhande makkelijke links zodat ze dat ook makkelijk weten te vinden. E geeft aan dat er twee manieren zijn waarop je standaard kunt communiceren met medewerkers en dat is het intranet en het nieuwsblad. E: 'Als mensen inloggen dan starten ze meteen op met de nieuwspagina van het intranet. De bevinding is wel dat het eigenlijk nooit gelezen wordt, dat wordt meteen weggeklikt. Maar goed het is een manier om te communiceren en dat is één kant. En we hebben een maandelijkse uitgave van ons nieuwsblad en daar staan dan zaken in en dat wordt wel gelezen en daarin hebben we dat ook onder de aandacht gebracht.

Ook heeft zorginstelling E stellingen ontwikkeld en die stellingen met antwoorden wil E sturen naar alle teammanagers, zodat het meegenomen kan worden in het teamoverleg: één stelling per keer per team. Bij deze teamoverleggen zitten bijvoorbeeld behandelteams en wijkteams. Vanuit de bestuursstaf wordt gezegd dat het onderwerp op de agenda moet, maar dit plan is nog in ontwikkeling. Zorginstelling E wil hier ook de intranetpagina aan koppelen door hier een toelichting op de stelling te geven.
Op dit moment wordt er in zorginstelling E al regelmatig gecommuniceerd over de procedures. Er wordt ook nagedacht over andere manieren om het onderwerp onder de aandacht te brengen.

De gekozen maatregelen worden regelmatig geëvalueerd
Incidenten worden gezien als leermomenten. E: 'Dus we gebruiken het om alerter te worden en om te ontdekken waar bijvoorbeeld zwakke plekken zitten in onze infrastructuur en dat kan leiden tot een advies van 'joh we moeten het anders gaan doen'. Een voorbeeld van zo'n incident is dat er 17 meldingen binnenkwamen dat er cliëntendossiers bij de printer bleven liggen. G: 'We hebben natuurlijk getoetst van hoe kan dat nou dat dat gebeurt want we hebben toch de mogelijkheid om beveiligd te printen. Maar ze kunnen kiezen om dat niet te doen en dan is de vraag van 'goh hoe breng je dat nu onder de aandacht van 1800 medewerkers?'

Het beleid wordt na evaluatie indien nodig aangepast
Het advies van E op het incident van de cliëntendossiers bij de printer is een proefconcept voor follow-me printen. Mensen hebben dan maar één printer en kunnen niet meer kiezen.

7.6 Analyse zorginstelling F

Actieve betrokkenheid van het bestuur
Ideeën over dit thema komen over het algemeen bij F vandaan. Toen bijvoorbeeld de Wet Meldplicht Datalekken werd ingevoerd heeft F een document opgesteld en deze aan de Raad van Bestuur gegeven met daarbij de opmerking: 'volgens mij moeten we dit en dit gaan doen'. Soms komt het ook bij de Raad van Bestuur vandaan als zij iets signaleren of een vraag binnenkrijgen. Het is dus tweerichtingsverkeer.
Het bestuur van zorginstelling F is dus wel betrokken, maar niet actief betrokken door bijvoorbeeld deel te nemen aan een privacyteam.

Prioriteit van privacy in organisatie
Zorginstelling F is al zes jaar bezig met privacy. Ieder jaar is het een terugkerend thema. Privacy heeft dus al langere tijd prioriteit in zorginstelling F.

Er is een risico-inventarisatie gedaan
Het belangrijkste is dat alle patiënten erop moeten kunnen vertrouwen dat hun gegevens bij zorginstelling F in goede handen zijn, dus dat willen ze uitstralen. Dit is lastig in een ziekenhuis, omdat iedereen naar binnen kan lopen. De Raad van Bestuur wordt daarnaast ook wakker als ze weten dat ze kans hebben op een boete van 820.000 euro.

Risico's van een beveiligingsissue zijn in beeld bij bestuur
De Raad van Bestuur heeft de gevolgen goed in beeld. Los van die boete heb je als organisatie ook een klus die je moet uitvoeren als je met een datalek van doen hebt. Je moet ontdekken wat de oorzaak van het lek is, wat de gevolgen van het lek zijn en wat je daaraan kunt doen. Daarnaast heb je herstelwerkzaamheden als ziekenhuis om aan het basisprincipe te kunnen voldoen dat iedere patiënt op je moet kunnen vertrouwen. Naast het risico op een boete, erkent het bestuur ook andere risico's zoals dat je patiënten hun vertrouwen in je organisatie verliezen.

Er is op basis van risico-inventarisatie een beleidsdocument informatiebeveiliging opgesteld
F geeft aan dat informatiebeveiliging drie kenmerken heeft: beschikbaarheid, betrouwbaarheid en vertrouwelijkheid. F is verantwoordelijk voor al het beleid omtrent informatiebeveiliging.
Er worden ook veiligheidsrondes gedaan waar F ook in meeloopt. F kijkt dan of er dingen zijn op het terrein van informatiebeveiliging of privacy die verbetering behoeven. Voorbeelden hiervan zijn papierkratten of computers die open staan, terwijl deze eigenlijk netjes vergrendeld moeten worden. Dit weet ook iedereen bij zorginstelling F, daar zijn gedragsregels over afgesproken.

In zorginstelling F heerst een aanspreekcultuur. Dat betekent dat medewerkers opletten wat er gebeurt en elkaar erop aanspreken wanneer je dingen ziet waarvan je denkt dat dit anders hoort. Niet met het idee van dat je iets fout gedaan hebt, maar meer van joh denk er even aan. Er heerst hierbij een open sfeer.
F heeft een actielijst opgesteld met wat er in de komende tijd uitgevoerd moet worden. De Privacy Impact Assessments gericht uitvoeren is bijvoorbeeld nog een stap die zorginstelling F nog goed in zijn proces moet inpakken.

Er wordt regelmatig gecommuniceerd over het informatiebeveiligingsbeleid
F geeft voorlichting en adviseert F gevraagd en ongevraagd. Daarbij beweegt F zich door de hele organisatie, dus vanaf de werkvloer tot aan de Raad van Bestuur.
Normaal gesproken houdt F een presentatie voor nieuwe medewerkers waarin F aangeeft wat de instelling van nieuwe medewerkers verwacht. Nu is er net een film gemaakt voor nieuwe medewerkers die de eerst volgende bijeenkomst wordt laten zien. Ook gaat F bij de afdelingen langs en doet F presentaties over informatiebeveiliging, privacy en de Meldplicht Datalekken.
Zorginstelling F is al zes jaar aan de slag met communiceren rondom informatiebeveiliging. Het is ieder jaar een terugkerend thema. Er wordt op dezelfde manier naar iedereen gecommuniceerd. F is van mening dat het niet uitmaakt wat je in de organisatie doet, voor iedereen gelden dezelfde regels. Daarom vindt F dat iedereen op dezelfde manier geïnformeerd moet worden over wat er van medewerkers verwacht wordt.
F is bekend met de 'ZEKER' campagne van de NVZ, omdat die komt uit het netwerk informatiebeveiliging waar F ook lid van is. F doet zelf altijd in de weken van Alert Online de informatieveiligheidsmarkt en dan zie je ook de campagne 'ZEKER' voorbij komen. Hij haakt hier dan op in. Eén van de onderdelen van de informatieveiligheidsmarkt was bijvoorbeeld het invullen van de zekertest. Deze test kon je ter plekke invullen met een groot scherm zodat mensen konden meekijken.
Er wordt door zorginstelling F op verschillende manieren gecommuniceerd zowel persoonlijk als via media.

Er wordt gewerkt aan het verhogen van beveiligingsbewustzijn in de organisatie
F doet bewustwordingscampagnes. Hij betrekt hier wel andere mensen bij zoals bijvoorbeeld de communicatieafdeling.
In 2011 is bijvoorbeeld een campagne gelanceerd waarbij door de hele instelling 300 gele vogeltjes zijn opgeplakt, zonder dat daar verder enige vorm van communicatie over is gedaan. Een week later zijn de vogels weer weggehaald en tot de maandag daarop is hier niks over gecommuniceerd. Mensen in de organisatie haakten op de campagne in door vogelgeluiden als achtergrondgeluid in te stellen. Het idee achter deze campagne was dat er juist reuring moest gaan ontstaan en dat mensen zich af gingen vragen wat die vogeltjes daar deden. De week erop is een poster verspreid met een geanonimiseerde dokter daarop. Je zag deze dokter een gesprek voeren per telefoon door de galerij waar in principe andere mensen dit gesprek konden horen. Op de poster stond een balustrade met daarop het kleine gele vogeltje. Deze werd ingezet als luistervink met de centrale boodschap: we hebben hier een luistervink en voor je het weet luistert of kijkt deze mee. Deze luistervink wordt ingezet als symbool voor informatiebeveiliging.
F komt nog voldoende mensen tegen die getraind moeten worden in het herkennen van phishingmails. Een mooi voorbeeld als onderdeel van de bewustwording was een bericht op intranet over ransomware. Vlak na dit bericht heeft zorginstelling F een phishingmail uit laten gaan. Als je goed naar deze mail keek zag je dat de afzender niet de stafdienst ICT was en als je goed naar de link keek zag je dat dat ook geen zuivere koffie was. Toch hadden best veel mensen op deze mail geklikt. Zo'n bewustwordingscampagne in de vorm van zo'n mail helpt alleen al om mensen scherp te maken.
Zorginstelling F kiest een paar momenten per jaar uit voor een bewustwordingscampagne. De ene keer pakken ze het iets groter aan dan de andere keer. Er wordt dus herhaaldelijk gewerkt aan het vergroten van beveiligingsbewustzijn en op verschillende manieren.

Er zijn duidelijke procedures aanwezig voor het behandelen van beveiligingsincidenten
Zodra je een datalek constateert is eigenlijk het eerste wat je moet doen zorgen dat F het weet. Medewerkers kunnen intern bij F melden. Dit weten zij onder andere door de presentaties van F. Daarnaast is het onderdeel van de procedure die vindbaar is op het kwaliteitsportaal. Toen zorginstelling F die procedure heeft gepubliceerd, heeft de instelling dit ook in de lijn gecommuniceerd aan lijnverantwoordelijken die dat weer door kunnen zetten naar de rest van de lijn. Op deze manier is geprobeerd dit zo breed mogelijk op het netvlies te krijgen in de organisatie. Er zijn twee methodieken om een datalek te melden je kunt F mailen of bellen of

iemand meldt een incident bij de helpdesk waarbij de melder nog niet doorheeft dat het om een datalek gaat. De helpdesk heeft de instructie om bij ieder incident na te gaan of dit een potentieel datalek is en kan dan een vinkje zetten als dit zo blijkt te zijn. Dan krijgt F dit via het systeem door. F is 24 uur per dag beschikbaar voor datalekken.
Er is dus duidelijk hoe je een melding moet doen bij zorginstelling F. Er zal nog wel iets duidelijker mogen worden wat de procedure precies inhoudt en wat F als vervolgstappen neemt na het krijgen van een melding.

Er wordt regelmatig over deze procedures gecommuniceerd
Zorginstelling F heeft een intranet, maakt gebruik van nieuwsbrieven en van postercampagnes. Daarnaast houdt F één keer per jaar een informatiebeveiligingsmarkt waarin ook privacy aan de orde komt. Dit jaar ging dit ook specifiek over de Meldplicht Datalekken. Deze markt houdt zorginstelling F voor de ingang van het restaurant, omdat daar veel medewerkers langslopen. Ze kondigen deze markt aan op intranet en kondigen het ook weer af op intranet door de highlights hierop te presenteren. Op deze manier worden ook mensen die die dag niet aanwezig waren op de hoogte gehouden. Maar daarnaast is het echt het belangrijkste om bij afdelingen langs te gaan en daar je verhaal te vertellen. Hier houdt F dan een verhaal over informatieveiligheid. F begint meestal met social media om aan te sluiten bij de werknemer en zijn privéleven en maakt vervolgens een bruggetje naar het werk. Centraal hierbij staat wat zorginstelling F van de medewerker verwacht po het gebied van informatieveiligheid.
F communiceert op verschillende manieren en herhaaldelijk over de procedures omtrent privacy.

De gekozen maatregelen worden regelmatig geëvalueerd
De evaluatie van de communicatie zou nog wel wat beter kunnen. F doet wel evaluatie met mensen die betrokken zijn geweest bij een bespreking en vraagt dan wel wat de betrokkenen goed en minder goed vonden werken, maar zorginstelling F vraagt de medewerkers niet specifiek om mee te evalueren. Na presentaties vraagt F ook wel om tips.

Het beleid wordt na evaluatie indien nodig aangepast
F heeft een actielijst met punten die aangepast moeten worden om te kunnen voldoen aan de AVG in 2018.

7.7 Analyse zorginstelling G
Actieve betrokkenheid van het bestuur
G zegt dat je informatiebeveiliging met de hele organisatie doet, maar dat ze het het liefst wel bij je weg stoppen en er het liefst zo min mogelijk mee te maken hebben. De functie zou eigenlijk rechtstreeks onder de Raad van Bestuur moeten zitten, maar zit nu bij ICT. G geeft altijd het advies of er wel of niet gemeld moet worden.
G schrijft het beleid, maar overlegt wel altijd met de Raad van Bestuur: ‘Ja, ik overleg altijd en ik adviseer altijd als ik het zelf geschreven heb om dat te accorderen zeg maar en als een ander dat geschreven heeft wat ik ervan vind en ook om het te accorderen. Ja, de Raad van Bestuur is daar altijd bij betrokken, die is ook hoofdelijk aansprakelijk.
Er is nog geen managementcommitment voor privacy: ‘Formeel nog niet nee. Ze weten zeker dat het de nodige aandacht heeft. Je hebt er continu discussie over, maar als je met de NEN en ISO bezig bent heb je echt managementcommitment nodig en het moet ook minimaal één keer per maand op de agenda staan en vastgelegd worden wat daar besproken is en ook wat de stukken zijn die aangeleverd moeten worden. Dat moet volgend jaar ook echt gaan gebeuren zeg maar’.
G geeft aan dat je wel merkt dat er wat meer aandacht is vanuit het management sinds de invoering van de Wet Meldplicht Datalekken. Met de nieuwe wetgeving en de consequenties daarvan is het ietsjes makkelijker geworden om acties te ondernemen.
G heeft regelmatig overleg met het bestuur en het bestuur is hoofdelijk aansprakelijk, maar er is nog niet echt commitment van het management.

Prioriteit van privacy in organisatie
G geeft aan dat er vorig jaar een risicoanalyse gedaan is en dat daar een aantal punten uit naar boven kwamen en dat toen gevraagd is vanuit de directie om dat op te pakken. Volgens G krijgt privacy de juiste prioriteit: ‘Het krijgt de juiste prioriteit ja. Ze zijn er zeker van bewust dat het impact heeft’. Dit kun je bijvoorbeeld zien aan dat er snel gereageerd wordt op mail en dat ook zij opvallende dingen doorgeven. Ook wordt onder

directeuren besproken wat er gebeurd is en dan wordt G in de loep gezet om te kijken hoe ze het lek kunnen afdekken en of er nog iets gemeld moet worden.

Er is een risico-inventarisatie gedaan
Er is in 2015 een risicoanalyse gedaan.
Over de risico's van een datalek zegt G: 'Dat ligt eraan op welk gebied het lek is of het een cliëntdossier is of alle cliëntdossiers dan haal je het acht uur journaal wel, we zijn natuurlijk een redelijk grote club. Dus ja dan heb je wel een probleem'.

Risico's van een beveiligingsissue zijn in beeld bij bestuur
Alle punten die er zijn gaan bij zorginstelling G sowieso altijd via het bestuur. De bestuurders zijn altijd op de hoogte van incidentmeldingen. G antwoordt op de vraag of de gevolgen goed in beeld zijn bij het bestuur: 'Nou ja goed zijn deze gevolgen in beeld bij het bestuur, ja dat ligt eraan of je een boete gaat krijgen of niet'. De gevolgen van de boete zijn dus wel goed in beeld bij het bestuur.

Er is op basis van risico-inventarisatie een beleidsdocument informatiebeveiliging opgesteld
G hield zich eerst bezig met architectuurvraagstukken. Met de nieuwe wetgeving is dat verder uitgebreid naar functionaris gegevensbescherming.
Het beleid van zorginstelling G is nog niet echt specifiek gericht op informatiebeveiliging: 'Er zijn sowieso gedragsregels. Niet specifiek voor informatiebeveiliging op dit moment. Er is wel een soort van protocol waarin de standaardzaken staan, maar dat is echt niet veel bijzonders. Dat is dat je elkaar moet aanspreken op een aantal zaken, usb en dat soort dingetjes, clean desk, nou dat zijn een beetje de standaard punten'.
In aanloop naar de AVG wil G op de NEN-manier gaan werken: 'Door te zorgen dat je op de NEN-manier werkt dat je dat geadopteerd hebt en dat je volgens die weg werkt dat je je managementsysteem op orde hebt. Het zijn iets van 135/140 controls die je als organisatie moet beantwoorden hoe je daarmee omgaat. Dus die moet je één voor één af en dan aan de hand van de businessimpact en de risicoanalyse kan je ze kwalificeren en dan kan je zeggen degenen die het meeste pijn doen alvast behandelen en zorgen dat je dat op orde hebt'.

Er wordt regelmatig gecommuniceerd over het informatiebeveiligingsbeleid
Er is een samenwerking met communicatie voor het communicatievlak. G: 'We hebben laatst geflyerd met een aantal speerpunten en ook materiaal rondgemaild. Nieuwsbrieven doen we en we zorgen dat het dan op alle locaties ligt op plekken waar mensen komen'.
Ook wordt er geïnformeerd aan medewerkers dat ze dossiers niet mee mogen sturen via de mail: 'Ja, ja zeker. Ze weten ook dat het niet mag'.
Er wordt onderscheid gemaakt tussen extramuraal en intramuraal in communicatie. G: 'Dat zit anders in elkaar. Extramuraal loopt iedereen met Ipads of met dossiers op de fiets. Die komen echt bij de mensen thuis dus daar spelen wat andere dingen dan bij de teams die binnen zitten, wat in principe afgesloten ruimtes zijn. Ja dan werkt het net iets anders'.
De flyercampagne die werd ingezet was de 'ZEKER' campagne van de NVZ. De online test hebben ze niet gebruikt, omdat die leek op de training die ze zelf hebben lopen.
Er wordt op verschillende manieren gecommuniceerd over informatiebeveiligingsbeleid.

Er wordt gewerkt aan het verhogen van beveiligingsbewustzijn in de organisatie
Er is een awarenesstraining bij zorginstelling G die verplicht is om te doen door iedereen. Hij is verplicht voor nieuwe medewerkers en huidige medewerkers moeten hem voor het eind van het jaar gedaan hebben. G: 'Ja, het is een online training voor awareness, voor informatiebeveiliging. Dus het zijn iets van 20 punten geloof ik waar je gevraagd wordt wat wel of niet goed is en als je antwoord heb gegeven dan staat erachter een verklaring van waarom dat zo is met wat verdere tekst en uitleg'.
De awarenesstraining getuigd van het werken aan het vergroten van beveiligingsbewustzijn in zorginstelling G.

Er zijn duidelijke procedures aanwezig voor het behandelen van beveiligingsincidenten
Er is een intern meldpunt en dat komt bij G uit. Ook is er één keer per maand een inloopspreekuur voor als mensen vragen hebben. Het doen van meldingen is nog niet in het systeem geïntegreerd, maar daar zijn ze wel mee bezig om dat voor elkaar te krijgen. Medewerkers weten volgens G waar en hoe ze moeten melden dat is gepubliceerd en regelmatig gecommuniceerd.

Er is dus wel een intern meldpunt, maar het is nog niet in het systeem geïntegreerd.

Er wordt regelmatig over deze procedures gecommuniceerd
Er is geïnformeerd aan medewerkers dat de wet er is. G: 'Dat is via de directeuren gegaan dat dat naar hun afdeling en mensen bekend is en daar flyeren we ook voor en daar sturen we mailtjes voor, de nieuwsbrief en op de intranetpagina staan daar regelmatig stukken over van ja waar je je aan moet houden. G geeft aan dat dit ook onderdeel is van de awarenesscampagne.
Middels presentaties probeert G ook de kwaliteitsafdeling mee te nemen in het verhaal. Hij wil informatiebeveiliging onderdeel maken van het werkproces en zorgen dat daar ook gemeld kan worden en dat zij ook acties uit gaan zetten.
Er wordt op verschillende manieren over de procedures gecommuniceerd.

De gekozen maatregelen worden regelmatig geëvalueerd
Er komen vanuit de organisatie vragen over waarom iets zo is als dat het aangegeven is of dat het eigenlijk veels te makkelijk is. Daar probeert zorginstelling G wel van te leren en je krijgt daar wel discussies over onderling. Ook naar het management toe dat er dingen anders moeten zoals het gebruik van Whatsapp.

Het beleid wordt na evaluatie indien nodig aangepast

7.8 Analyse zorginstelling H

Actieve betrokkenheid van het bestuur
De afdeling privacybescherming en informatiebeveiliging stelt het beleid op. H1: 'Maar wij mobiliseren onder andere natuurlijk dat hele netwerk en de rest van de organisatie en we zorgen ook dat we de opdracht hebben in feite ook van de Raad van Bestuur, maar wat eruit komt, dus het informatiebeveiligingsbeleid daar staat natuurlijk de Raad van Bestuur vierkant achter en wij doen alleen mensen bij elkaar brengen en zorgen dat het op papier komt'. H1 geeft aan dat de Raad van Bestuur het thema volledig in beeld heeft. H1: 'Daarom zijn wij ook benoemd en geregistreerd. De Raad van Bestuur heeft dit als vast onderwerp en één van de leden van de Raad van Bestuur heeft dit ook in zijn portefeuille en daar hebben wij ook regulier overleg mee en wij moeten ook op regelmatige basis rapporteren aan de Raad van Bestuur hoe de zaken ervoor staan'.
De Raad van Bestuur is uiteindelijk degene die bepaalt of iets gemeld wordt.
Er vindt regulier overleg plaats met de Raad van Bestuur en de Raad van Bestuur bepaalt of iets gemeld wordt ja of nee. Er is dus een zeer actieve betrokkenheid van de Raad van Bestuur in zorginstelling H.

Prioriteit van privacy in organisatie
Er is een afdeling privacybescherming en informatiebeveiliging. In dit team zitten vier personen. Hierin drie FG's bij elkaar en één iemand die is documentalist. H2 zit in de divisie waar onderzoek plaatsvindt en H1 zit bij bestuurlijke en juridische zaken, dus het bureau van de Raad van Bestuur.
Er is ook een incident geweest bij zorginstelling H een tijdje terug en daardoor is privacybescherming hoog op de prioriteitenlijst gezet.
Toon het top is volgens H2 erg belangrijk. H2: 'Nou de hoogste top is zeker wat betreft privacy en informatiebeveiliging bij de les. Dat stralen ze ook uit. Dat is al één randvoorwaarde. Maar we spreken nu ook duidelijk de hele lijn aan dus afdelingshoofden en werkplekmensen op hun verantwoordelijkheid daarin'.
De Raad van Bestuur geeft ook aan dat er consequenties verbonden moeten worden aan het niet naleven van de regels.
Mede dankzij het incident een aantal jaar terug staat privacy nu hoog op de prioriteitenlijst bij zorginstelling H.

Er is een risico-inventarisatie gedaan
Gebrek aan awareness is volgens zorginstelling H een heel groot risico.H1: 'Dat merken wij ook als we incidenten afhandelen: hoe halen ze het in hun hoofd om dit gedaan te hebben?'
H1 geeft aan dat er nu wel risico-inventarisaties gedaan worden, maar dat dit nog onderdeel moet worden van de integrale bedrijfsvoering.

Risico's van een beveiligingsissue zijn in beeld bij bestuur
H1 geeft aan dat de Raad van Bestuur de risico's heel goed in beeld heeft. Het onrechtmatig raadplegen van gegevens is bijvoorbeeld een risico. H1: 'In zijn algemeenheid geldt hè als je kijkt naar de risico's waarvan ze

zeggen: ojee daar komt ellende uit. Op nummer 1 staat met stipt het gebrek aan awareness waardoor mensen in kennis gehinderd fouten maken en daardoor incidenten veroorzaken. En waarvoor wij eigenlijk nog het meest beducht zijn dat is reputatieschade'.
Er zijn dus verschillende risico's van een beveiligingsissue in beeld bij het bestuur.

Er is op basis van risico-inventarisatie een beleidsdocument informatiebeveiliging opgesteld
Toezichthouden, adviseren en awareness zijn de kerntaken voor de afdeling privacybescherming en informatiebeveiliging. H2: 'We werken dus ook in een netwerk met mensen die zich daarmee bezighouden, dus informatiebeveiliging wat veel technische kanten heeft, samen met de technical security officer van de ICT-afdeling, maar ook met het Hoofd Veiligheid als het gaat om fysieke gegevens en dergelijke'. H1 geeft aan dat het netwerk eigenlijk nog groter is. Ze werken ook met bedrijfsjuristen en gezondheidszorgjuristen samen.
Zorginstelling H wil de NEN7510 norm geïmplementeerd hebben voor informatiebeveiliging.
Privacybescherming en informatiebeveiliging moeten onderdeel zijn van de reguliere bedrijfsvoering. Het moet onderdeel worden van de plan-do-check-act cyclus. Een voorbeeld hiervan is deelnemen aan de reguliere interne audits dat privacy en informatiebeveiliging daar onderdeel van worden.
Er zijn ook maatregelen bij het niet naleven van regels. Zorginstelling H doet onder andere aan login-opvolging. H1: 'Er is nu een complete brief in de maak, die naar iedereen gaat die vertrouwelijke gegevens moet raadplegen, die krijgen het op de deurmat. Daar staat ook in inderdaad dat er spelregels zijn en dat als ze zich daar niet aan houden dan kan dat rechtspositionele consequenties hebben, zoals een disciplinair gesprek tot en met ontslag. De Raad van Bestuur zegt: we gaan hieraan echt consequenties verbinden'.

Er wordt regelmatig gecommuniceerd over het informatiebeveiligingsbeleid
Er is een vast contactpersoon bij communicatie die ook in de commissie privacybescherming en informatiebescherming zit. Communicatie heeft ook een prachtige site gemaakt voor privacybescherming en informatiebeveiliging. Alle uitingen die gemaakt worden in het kader van awareness lopen via dit vaste contactpersoon.
Zorginstelling H heeft ook gedeeltelijk meegedaan aan de 'ZEKER' campagne van de NVZ. H1: 'Er zijn een aantal berichten via de reguliere media het huis ingegaan om de privacybescherming te bevorderen op basis van die campagne. Maar die campagne werd door ons niet als heel erg adequaat bestempeld'.
Zorginstelling H wil ook e-learningmodules op het gebied van privacybescherming en informatiebeveiliging ontwikkelen die verplicht worden voor alle medewerkers, maar wel wat meer toegesneden op de groepen, omdat informatiebeveiliging en privacybescherming iets anders betekenen voor mensen in de zorg als voor mensen op ondersteunende afdelingen of voor onderzoekers.
H2 wil meer heen naar pakketjes aanbieden aan de contactpersonen informatiebeveiliging en privacybescherming zodat die pakketjes in werkoverleggen gebruikt kunnen worden.
Op het intranet plaatst ICT bijvoorbeeld ook regelmatig berichtjes over ransomware, maar dat wordt slecht gelezen. H1: 'Maar de effectiviteit daar hebben wij grote twijfels over'.
Er wordt op verschillende manieren gecommuniceerd over het informatiebeveiligingsbeleid en er wordt nagedacht over hoe communicatie het beste kan werken.

Er wordt gewerkt aan het verhogen van beveiligingsbewustzijn in de organisatie
In zorginstelling H wordt gewerkt aan het verhogen van beveiligingsbewustzijn. H1: 'We hebben sowieso van die posters, do's en don'ts, we doen gebouwrondes. Iedere twee maanden doen we zo'n gebouwdeel en dan leggen we een soort kaarten neer met smileys met achterop wat wel en wat niet kan. We merken dat dat een heel sterk awareness bevorderend effect heeft, want als we ergens een ronde gedaan hebben, worden we meteen heel vaak gebeld van waarom dat zo is. En daarnaast zie je die kaarten her en der. We hebben twee sites voor informatiebeveiliging en privacybescherming één voor gebruik van social media. Bij binnenkomst in de organisatie krijgen nieuwe medewerkers ook een praatje.
Als er een issue is wordt er gecorrespondeerd met afdelingen en bij dingen als een datalek komt het ook in het weekblad. Als er ernstige incidenten zijn dan besteedt zorginstelling H daar aandacht aan en plaatsen ze weer een artikeltje om de awareness te bevorderen.
De e-learning draagt ook bij aan het verhogen van beveiligingsbewustzijn.
Zorginstelling H heeft ook contactpersonenbijeenkomsten. Iedere afdeling heeft een contactpersoon informatiebeveiliging en privacybescherming. H1: 'Daarvoor organiseren we kwartaalbijeenkomsten om allerlei onderwerpen te bespreken. Dat zijn eigenlijk onze ambassadeurs op de afdelingen'.

Er wordt geen onderscheid gemaakt tussen verschillende groepen in communicatie.
Er wordt op verschillende manieren gewerkt aan het verhogen van beveiligingsbewustzijn in zorginstelling H. Ook wordt er herhaaldelijk aandacht aan besteed.

Er zijn duidelijke procedures aanwezig voor het behandelen van beveiligingsincidenten
Meestal nemen medewerkers rechtstreeks contact op met H1 of H2. Maar er zijn verschillende elementen ingericht voor de signalering. Er kan gebeld worden, mensen kunnen mailen, er is een meldsysteem daarin staan ook een aantal vragen naar een datalek, er kan een melding via de receptie of beveiliging binnenkomen bij bijvoorbeeld een gestolen laptop. Ook kunnen datalekken binnenkomen via social media en via de helpdesk ICT. H1: 'Dan doen wij de eerste beoordeling en indien het een ernstig incident is dan nemen wij meteen contact op met de secretaris van de Raad van Bestuur dan vind er een beoordeling plaats en dan wordt gekeken of we dat in een kleine setting kunnen afhandelen. Dat betekent wij toetsen aan de wet en kijken of we melding moeten doen aan de AP en of betrokkenen geïnformeerd moeten worden en dergelijke en op die manier geven we een advies en dat neemt de Raad van Bestuur dan over of niet en wij zorgen dat het uitgevoerd wordt, maar bij een ernstig incident wordt het hele circus opgetrommeld. Iemand uit de Raad van Bestuur wordt de voorzitter van de beheersgroep. Daar zit ook de directeur communicatie en daar zit de voorzitter van de commissie privacybescherming in en daar zitten wij in en daar zit de directeur ICT bij en de technical security officer die kennis heeft van de harde informatiebeveiliging dus heel technisch. En dan komen we afhankelijk van de ernst: één of meerdere keren per dag bij elkaar zal ik maar zeggen. En dan wordt daar netjes verslag van gemaakt en we bouwen een dossier op. De procedure is eigenlijk heel kort en krachtig. Het zijn eigenlijk maar drie velletjes en dat is ook eigenlijk de kracht van de procedure iedereen weet meteen wat hij moet doen en wij zijn eigenlijk degenen die dan het proces sturen'.
De procedures van zorginstelling H zijn erg gedetailleerd en het is duidelijk op welke verschillende manieren medewerkers van zorginstelling H kunnen melden.

Er wordt regelmatig over deze procedures gecommuniceerd
Er is hierover niet gesproken tijdens het interview. Zorginstelling H doet dus niet mee op dit punt. Aangenomen mag worden dat er ook hierover gecommuniceerd wordt als gekeken wordt naar het uitgebreide pakket aan communicatiemaatregelen voor de andere punten.

De gekozen maatregelen worden regelmatig geëvalueerd
Incidenten worden wel geëvalueerd en er worden interne en externe audits gedaan.

Het beleid wordt na evaluatie indien nodig aangepast

7.9 Analyse zorginstelling I

Actieve betrokkenheid van het bestuur
I heeft een nulmeting laten doen voor het hele bedrijf en die ligt nu bij de Raad van bestuur maar daar gebeurt niks mee op dit moment. Het bestuur heeft het thema wel in beeld, maar ze acteren nog niet echt. I: 'Ja, de Raad van Bestuur is er maar één dus die heeft niet eens een portefeuille. De Raad van Bestuur is één iemand. Maar de Raad van Toezicht zal dit ook op zijn agenda moeten hebben, alleen daar ligt het nog niet omdat het bestuur daar niet neerlegt'. Zorginstelling I krijgt binnenkort een nieuwe bestuurder, dat kan een mogelijke verklaring zijn waarom deze dingen blijven liggen. Er is op dit moment dus geen actieve betrokkenheid van de Raad van Bestuur en er zijn ook geen plannen van het bestuur om wel betrokken te raken.

Prioriteit van privacy in organisatie
Alle documenten liggen ter goedkeuring bij de Raad van Bestuur en de Raad van Bestuur doet hier niks mee. Er is dus geen hoge prioriteit van privacy in de organisatie. I geeft aan dat er wel communicatiemiddelen beschikbaar zijn maar dat privacy en security gewoon niet op de agenda staat: 'Ja dat hebben we allemaal wel, we hebben ook gewoon een leerportaal en trainingen en dat soort zaken. Het is allemaal wel beschikbaar maar privacy en security staan gewoon niet op de agenda. Dus als het niet over zorg of over medische handelingen gaat dan is er gewoon geen interesse voor wat ik wel snap'. Er is dus geen prioriteit voor privacy in zorginstelling I en er zijn ook geen plannen om hier verandering in aan te brengen.

Er is een risico-inventarisatie gedaan
Er is een nulmeting gedaan door een extern bedrijf.
I: 'ons grootste risico is dat er cliëntdossiers op straat komen te liggen. Ja, aan de andere kant is dat ook weer niet zo'n heel groot risico. Als het gebeurt hebben we een ernstig probleem, maar de kans dat het gebeurt is niet zo heel groot'.
Er zit een risicoanalyse en een dreigingsanalyse in het NEN-7510 project.

Risico's van een beveiligingsissue zijn in beeld bij bestuur
De risico's zijn niet echt goed in beeld bij de Raad van Bestuur: 'Nou ze zijn zich er vaag wel van bewust, maar ze denken ook dat zal mijn tijd wel doen en het gebeurt toch niet'. De Raad van Bestuur is zich dus wel vaag bewust van risico's, maar acteert er niet op.

Er is op basis van risico-inventarisatie een beleidsdocument informatiebeveiliging opgesteld
I is bezig met het NEN-7510 project. I wil dat de komende twee kwartalen echt gaan uitrollen. I: 'Daar komt ook een datalekprotocol in en een commissie en vaststellen wie doet wat en wanneer en die awarenesscampagne waarin ik privacy gewoon meeneem dus ja dat gaat binnenkort wel allemaal gebeuren dat wel'.
Er is al jarenlang een project geïdentificeerd om NEN-7510 gecertificeerd te worden, maar er is nu ook externe ondersteuning bij ingeroepen. I: 'We implementeren een managementtool daarvoor die de auditors en de maatregelen die daaruit komen echt monitort en op regelmatige basis ook bij stakeholders neerlegt. Dus het is eigenlijk een tool waar je die hele NEN-norm instopt en daar maak je dreigingsanalyses en impactanalyses en daar komen maatregelsets uit en die maatregelen koppel je weer terug aan stakeholders in het bedrijf. En die tool die monitort dan de plan-do-check-act-cyclus van al die maatregelen bij al die stakeholders'.
Het privacyreglement en gedragscodes liggen allemaal ter goedkeuring bij de Raad van Bestuur.
Het NEN-7510 project zal bestaan uit de volgende stappen: 'Opleveren van het informatiebeveiligingsbeleid, de processen en documentatie, het uitvoeren van de assessments en de analyses, de overdracht van kennis en kunde, het implementeren van maatregelen en de controle op de naleving van de certificering en daar zit wel veel in en we hebben een nulmeting gedaan op privacy dus dat is net weer even een iets andere insteek en daar zit ook een enorme lijst aan activiteiten in. Verkrijgen van inzicht in de verwerkingen en het benoemen van de eigenaren, beoordelen of er sprake is van een gezamenlijke verantwoordelijkheid, functieprofiel opstellen voor een FG, functieprofiel voor security officer, voldaan aan informatieplicht'.

Er wordt regelmatig gecommuniceerd over het informatiebeveiligingsbeleid
Er zijn nog geen ideeën over hoe medewerkers bereikt gaan worden. Zorginstelling I scoort daarom een 1 op dit punt.
I is niet bekend met de 'ZEKER' campagne van de NVZ.

Er wordt gewerkt aan het verhogen van beveiligingsbewustzijn in de organisatie
Zorginstelling I gaat en bedrijf selecteren voor een awarenesscampagne en dat doet I samen met communicatie. Er is een plan voor een awarenesscampagne, maar het wordt nu nog niet uitgevoerd.

Er zijn duidelijke procedures aanwezig voor het behandelen van beveiligingsincidenten
I is bezig met de procedure op poten te zetten. I: 'Protocol datalekken en het formeren van een commissie en dat soort dingen dat ben ik nu allemaal aan het doen'. Er is al wel een protocol opgesteld, maar deze wordt nog niet actief gebruikt.

Er wordt regelmatig over deze procedures gecommuniceerd
I geeft aan dat medewerkers helemaal niet eens weten dat de Wet Meldplicht Datalekken er is. Zorginstelling I heeft wel een intranet, een leerportaal en trainingen en dat soort zaken, maar allemaal niet op het gebied van privacy en security.

De gekozen maatregelen worden regelmatig geëvalueerd
Er zijn op dit moment geen mensen in zorginstelling I die erop toezien of het reglement goed wordt uitgevoerd.

Het beleid wordt na evaluatie indien nodig aangepast

7.10 Analyse zorginstelling J

Actieve betrokkenheid van het bestuur
Op dit moment hebben de leden van de Raad van Bestuur alle drie het onderwerp privacy in hun portefeuille. J2: 'Nou alle drie doen ze het, maar ze willen het er ook niet over eens zijn wie het uiteindelijk gaat doen. Ze vinden het alle drie interessant'. J1: 'Nou ik denk ook wel het boeiende met dit onderwepr. Het raakt feitelijk alle bedrijfsonderdelen van je organisatie. Of het nu gaat om patiëntgegevens, personeel, loongegevens of gewoon je bedrijfsinformatie het raakt echt overal. Dus ik snap daarom wel de behoefte van de bestuurders om een gemeenschappelijke betrokkenheid te hebben'.
De Raad van Bestuur keurt beleid goed., maar J1 stelt beleid op.
J1 rapporteert als het nodig is aan de Raad van Bestuur.
De Raad van Bestuur is dus actief betrokken en wil ook graag actief betrokken zijn bij het onderwerp.

Prioriteit van privacy in organisatie
J1 functionaris gegevensbescherming en J2 security officer vallen beiden direct onder de Raad van Bestuur en de afdeling waar ze zitten hangt af van hoe de Raad van Bestuur de portefeuilles verdeeld. Volgens J2 neemt de Raad van Bestuur privacy als onderwerp wel serieus. Ook is de Raad van Bestuur bereid om externen in te zetten om J1 en J2 te ontzorgen. De prioriteit van privacy is hoger dan dat het was volgens J1, J2 zegt een hoge prioriteit: 'Het staat in het risicoprofiel van de organisatie, daarin is het ook benoemd. Ze hebben het vorige week maandag met het MT besproken en toen werd er ook nadrukkelijk gezegd van is het wel nadrukkelijk genoeg beschreven, moeten we het niet wat hoger nog op de prioritering zetten? Cybercrime staat er ook op. Dus het is de combinatie van de dreiging en wat je verplicht bent om te doen en die combinatie maakt dat men het dus hoog op de agenda heeft staan'.
Teammanagers die vinden het soms maar onzin, je hebt ook managers die nog steeds zeggen van hè nou moet dat allemaal en wat krampachtig.
Er is volgens J1 en J2 wel prioriteit voor privacy in de organisatie, alleen teammanagers vinden het soms maar onzin.

Er is een risico-inventarisatie gedaan
Er is een risico-inventarisatie gedaan.
Identiteitsfraude is één van de grootste risico's van een datalek.

Risico's van een beveiligingsissue zijn in beeld bij bestuur
De Raad van Bestuur wil sowieso geen datalek, omdat je vertrouwen wilt en je geen imagoschade wilt. Je wilt ook niet dat dingen op straat komen te liggen. Er worden andere thema's dan de boete genoemd als risico's.

Er is op basis van risico-inventarisatie een beleidsdocument informatiebeveiliging opgesteld
Zorginstelling J heeft privacybeleid, een privacyreglement en allerlei aanverwante zaken zoals camerabeleid, autorisatie en toegangsbeleid. J1: 'Maar als het dan aankomt op jouw deel communicatie dan hebben we daar eigenlijk nog niet zoveel over.
Zorginstelling J heeft een nulmeting laten doen op hun privacybeleid en daar kwamen ook communicatiedingen uit, zoals een privacycontactpersoon aanstellen op de afdelingen.

Er wordt regelmatig gecommuniceerd over het informatiebeveiligingsbeleid
Medewerkers krijgen twee brochures bij indiensttreding: één over de samenvatting van de huisregels informatieveiligheid, waarvan privacy een onderdeel is. En één algemeen over wat informatieveiligheid is.
Alle serviceassistenten hadden vorig jaar een training en alle nieuwe medewerkers krijgen een introductiedag.
J1 geeft aan dat het niet voldoende is: 'Je merkt dat het ook herhalen is, praktische voorbeelden blijven benoemen en het is een taai onderwerp, het is absoluut niet sexy'.
J2 doet veel werkoverleggen. J2: 'Dan nodigen ze je uit en dan doen we een stukje voorlichting en onderricht en dat is een halen brengen verhaal. Want ik vertel wat over wat ons beleid is, hoe het zou moeten, waar aandacht voor zou moeten zijn en je haalt ook, want je hoort ook incidenten, je hoort ook waar ze tegenaan lopen en dat kun je weer meenemen in je beleid, dus daar zijn die werkoverleggen sowieso goed voor. Ik laat een Youtubefilmpje zien van hoe makkelijk je al je informatie op internet en hoe je daarbij kan komen en dan vertel ik gewoon even de grote lijnen van wat kun jij hier zelf doen en wat doen wij, wat proberen wij ook om

jou technisch te ondersteunen om het makkelijk te maken, dus bijvoorbeeld dit (laat zien hoe je en uitlogt door enkel je pasje te scannen) dat hadden we toen nog niet en nu hebben we dat wel en dat betekent dat ik ook verwacht dat iedereen heel snel in en uitlogt'.
Er is ook een pagina informatiebeveiliging op het intranet, die is gecommuniceerd aan de organisatie via de teammanagers en er is een e-learning die iedereen volgt.
De medische staf wordt bij zorginstelling J apart voorgelicht dat doet J2 minimaal 1x per jaar.
Zorginstelling J heeft meegedaan met de Alert Online campagne. J1: 'Hebben we ook met een kraampje bij het restaurant gestaan met folders en informatie en noem maar op en daar hebben we ook iedereen geattendeerd op de community en ga daar eens naar toe en daar zijn leuke vragen uit gekomen en foldertjes meegegeven'. J2: 'En we hebben ook in die week heel veel blogs geschreven, bijna dagelijks.
De samenwerking met de communicatieafdeling loopt bij zorginstelling J niet echt goed. Folders en dergelijke worden door J1 of J2 gemaakt. J2: 'Ik bedoel we hebben best creatieve ideeën waar we wel eens over nagedacht hebben, maar waarvan ik niet het gevoel heb dat ik dat kwijt kan en dat iemand het oppakt.
Er wordt op verschillende manieren gecommuniceerd over informatiebeveiliging, alleen de samenwerking met communicatie verloopt niet erg goed. Het moet vooral vanaf J1 en J2 komen.

Er wordt gewerkt aan het verhogen van beveiligingsbewustzijn in de organisatie
Er wordt wel gewerkt aan het verhogen van beveiligingsbewustzijn met behulp van e-learnings en voorlichting.

Er zijn duidelijke procedures aanwezig voor het behandelen van beveiligingsincidenten
Er zijn drie soorten meldingen: via de helpdesk, de meldingen die via J1 of J2 binnenkomen en de meldingen die voortkomen uit de VIM-meldingen. Ook kan het zijn dat een patiënt een klacht ingediend heeft bij het patiëntenservicebureau. J2 hoopt dat er volgend jaar een betere tool komt om die meldingen met elkaar te kunnen verbinden. Er wordt wel verteld welke manieren van melden er zijn, maar er wordt door zorginstelling J niet ingegaan op de specifieke procedure die daarna volgt.

Er wordt regelmatig over deze procedures gecommuniceerd
De procedures zijn via het intranet en via de nieuwsbrief gecommuniceerd. Zorginstelling J zit nu nog in de afronding van de nieuwe versie, want ze hadden al een procedure voor de wet. Ook wordt er vanaf het management naar de lijn gecommuniceerd en het komt terug in de voorlichting van J2. J2: 'Ja, iedere introductie zeg ik 'Meldplicht Datalekken' en als er een datalek is willen we worden gebeld, niet alleen gevimd, maar ook gebeld want dan moeten we binnen een bepaalde tijd handelen en nou ja dat gebeurt ook'.
Brochures is bij zorginstelling J nog wel een dingetje. J1: 'Brochures dat behoeft gewoon aandacht, daar moeten we echt nog wel een slag in maken'.
Er is op verschillende manieren gecommuniceerd over de procedures rondom datalekken.

De gekozen maatregelen worden regelmatig geëvalueerd
Bij de werkoverleggen hoor je waar medewerkers tegen aanlopen en dat kun je weer meenemen in je beleid. Ook bij incidenten wil zorginstelling J er graag van leren. Er komt altijd een werkoverleg na een incident. J2: 'Kijk wat je doet is eigenlijk zo van laten we nou met zijn allen leren van wat we fout hebben gedaan en laten we er vooral extra weer attent op zijn, want het gebeurt heel snel, heel makkelijk, onbedoeld ook. En dat is waar mensen werken, worden fouten gemaakt en daar kun je met elkaar van leren, maar het is wel altijd aanleiding om te zeggen van 'goh nou laten we dat dan even doen'.
J2 let ook wel op of ze alle afdelingen langs is geweest en of alle afdelingen iets doen aan informatiebeveiliging. J2: 'Dat hoort in onze plan-do-act-check cyclus te zitten dat we af en toe controle doen, maar ja dat is het eerste wat erbij inschiet. Maar dit soort dingen doe ik tegen het einde van het jaar voor het overzicht naar de Raad van Bestuur van wat is er nou gebeurd dan wil ik wel altijd even checken end an zijn er wel dingen die opvallen'.

Het beleid wordt na evaluatie indien nodig aangepast.

7.11 Analyse zorginstelling K

Actieve betrokkenheid van het bestuur

De divisies van zorginstelling K opereren redelijk zelfstandig. K: 'De Raad van Bestuur heeft een besturingsfilosofie waarbij eigenlijk heel veel verantwoordelijkheid in divisies zit, want daar hebben ze ook het beste inzicht hoe ze dingen moeten doen'.
Het team dat zich bezighoudt met informatiebeveiliging en privacy stelt het beleid op.
De meldingen naar de autoriteit persoonsgegevens doet het privacyteam namens de Raad van Bestuur.
Het bestuur is dus niet actief betrokken bij het privacybeleid.

Prioriteit van privacy in organisatie
K is in opdracht van de Raad van Bestuur op dit moment bezig om de hele informatiebeveiliging en privacybescherming beter vorm te geven. Op dit moment liggen informatiebeveiliging en de toezichthoudende rol beiden bij de staf van de Raad van Bestuur, maar hier komt waarschijnlijk een splitsing in. Er is een team informatiebeveiliging en privacy van twee man. De prioriteit van privacy is hoog bij de Raad van Bestuur: 'Het staat nu in de top 5 bij de Raad van Bestuur. Ze vinden het heel erg belangrijk en de verantwoordelijke in de Raad van Bestuur hamert er ook op bij mijn collega dat we stappen moeten maken. Wat kunnen wij nog meer doen? Hoe kan ik daar beter op sturen?'
K geeft aan dat er wel budget is maar dat dat vooral in de divisies ligt.
Privacy staat in de top 5 op de prioriteitenlijst van de Raad van Bestuur. Het heeft dus een hoge prioriteit. De Raad van Bestuur heeft ook aangegeven dat er een e-learningmodule moet komen.

Er is een risico-inventarisatie gedaan
De belangrijkste verstoringen zijn stroomstoringen, storingen in de infrastructuur en dat patiËnten hier niet meer kunnen komen. K: 'En als je dan gaat kijken naar ondersteunende informatiesystemen dan hebben we een aantal kernsystemen die mogen eigenlijk niet uitvallen'. Afgelopen drie jaar is zorginstelling K heel bewust bezig geweest met het doorvoeren van veel meer risicoanalyses.

Risico's van een beveiligingsissue zijn in beeld bij bestuur
Privacy staat in de top 5 van de Raad van Bestuur en laat daarmee zien dat er wel risico's aan verbonden zijn, welke risico's specifiek wordt niet duidelijk.

Er is op basis van risico-inventarisatie een beleidsdocument informatiebeveiliging opgesteld
K geeft aan hoe de structuur van informatiebeveiliging in elkaar zit: 'Elke divisie heeft een informatiemanager en de directies hebben er ook één en die worden ondersteund door een ICT-coördinator en functioneel beheerders, die hun eigen taken hebben in dat hele organisatieproces: het uitrollen van de middelen en het helpen van de eindgebruikers. De CISO-rol is heel breed: hoe bescherm ik de gegevens: wat voor maatregelen moet ik treffen, hoe communiceer ik daarover? En de FG heeft veel meer de rol van zijn die maatregelen effectief en doen we de juiste dingen? En als het fout gaat wat leren we ervan om te zorgen dat de gevolgen voor de betrokkenen beperkt blijven'.
Zorginstelling K heeft een informatiebeveiligingsbeleid en een stukje rondom privacy opgesteld en probeert steeds nieuwe stukjes tekst en beleid te vertalen naar iets wat het huis kan gebruiken.
Zorginstelling K heeft de NEN-7510 verder uitgewerkt naar meer concrete stappen die in het huis genomen kunnen worden. Dit omdat mensen in de zorg gewend zijn voorgeschreven te krijgen wat ze moeten doen. K: 'Dat stukje is voor iemand in de zorg lastig. Want die is namelijk gewend om te horen ik moet links of rechtsaf gaan in plaats van ik moet erover nadenken'.
Zorginstelling K heeft een sanctiebeleid. K: 'Als medewerkers bewust dingen doen die ze niet mogen doen, dan wordt vanuit de zorg gezegd hee wacht even dit zijn wel patiëntgegevens je was niet betrokken en hebt wel zitten kijken we gaan afscheid nemen'.

Er wordt regelmatig gecommuniceerd over het informatiebeveiligingsbeleid
Zorginstelling K heeft wel eens binnen het kader van de NVZ-campagne een bewustwordingscampagne opgezet: welk middel moet je inzetten en wat moet je niet doen? En wees bewust waar je op klikt. De directie zei hierover: 'Jullie hebben een aantal middelen en vertel die gebruikers nou eens een keer wat ze wel en wat ze niet moeten doen, want er zitten randvoorwaarden aan het gebruik van IT en communiceer daar een keer over'.
Ook voor patiënten is er informatie beschikbaar zoals een folder waarin staat wat je als patiënt kan verwachten en wat je niet kan verwachten.

Er wordt niet heel uitgebreid gecommuniceerd over het informatiebeveiligingsbeleid.

Er wordt gewerkt aan het verhogen van beveiligingsbewustzijn in de organisatie
Er wordt wel op afdelingen gesproken over privacy volgens K. Ook wordt de NEN-7510 vertaald naar concrete stappen voor de zorgsector en er komt een e-learningmodule. Er wordt dus op dit moment nog niet actief gewerkt aan het verhogen van beveiligingsbewustzijn in de organisatie, maar zorginstelling K is dit wel van plan.

Er zijn duidelijke procedures aanwezig voor het behandelen van beveiligingsincidenten
Er is een procedure meldplicht datalekken. K: 'De persoon die het ziet kan het bij ons melden via een aantal kanalen. Ze kunnen mailtjes sturen, ze kunnen ons opbellen, ze kunnen het melden in het incidentmeldingssysteem. Wij pakken de meldingen dan op, nemen contact op met die mensen, bepalen vervolgens met de informatiemanager van die divisie wat is er nou specifiek aan de hand en kijken vervolgens wat er moet gebeuren. Wij voeren de coördinatie op het hele traject om te kijken of wij de juiste dingen hebben gedaan. Melden we op tijd bij de Autoriteit Persoonsgegevens, melden we op tijd bij de betrokkenen, hebben we het goed voor elkaar en kunnen we daar ook bijspringen?'.
De UMC's proberen gezamenlijk een extern meldpunt te creëren.
De procedures rondom datalekken van zorginstelling K zijn duidelijk en ook het proces na de melding wordt duidelijk..

Er wordt regelmatig over deze procedures gecommuniceerd
De procedure Meldplicht Datalekken is via het bestuur gecommuniceerd. K: 'Dus we hebben wat teksten gemaakt voor de Raad van Bestuur. Dit komt eraan en wij verwachten dat wij dit en dit gaan doen als huis. Als er iets mis is, meld het aan bij ons'. Ook is K de eerste helft van het jaar de organisatie ingegaan met presentaties in de afdelingen bij MT's van de divisies om te vertellen wat informatiebeveiliging is en wat privacy betekent en wat je moet doen als iets niet goed gaat. Een aantal divisies hebben dit zelf opgepakt. K: 'Wij hebben het eerste half jaar geventileerd van jongens we willen graag wat vertellen over dit onderwerp. We hebben het MT benaderd, de Manager Bedrijfsvoering die dit in zijn portefeuille heeft en gezegd: 'u kunt zelf een presentatie geven of wij komen toelichting geven in een teamoverleg'. K geeft aan dat de divisies waar ze langs zijn geweest nu ook erg actief bezig zijn met informatiebeveiliging.
De afdeling marketingcommunicatie vormt de regie bij het omgaan met incidenten.
Een divisie mag zelf keuzes maken in de manier van communiceren. K: 'Er zijn bijvoorbeeld divisies die zeggen van doe voor ons een presentatie of een stukje tekst, maar we hebben een website waar we intern op kunnen publiceren, we hebben nieuwsbrieven die we kunnen publiceren. We hebben ook een centrale afdeling marketing en communicatie, die we voor twee dingen in kunnen zetten. Heel direct en persoonlijk gericht op de persoon: de medewerker, de patiënt, de student of veel meer algemeen naar de kranten toe, de pers. En dat zijn ook weer twee vormen die je kunt inzetten'.
De marketingadviseur heeft het huidige campagnetraject getrokken. K: 'Ze heeft dus een aantal dingen gemaakt die hier ook uitgedeeld zijn. Je ziet ze ook elektronisch, dus je kunt het nog opzoeken op het intranet'. Het is zo'n geplastificeerd a4tje met een aantal spelregels erop met wat doe je wel en wat doe je niet. En die zijn door het huis verspreid en het is ook op de website geplaatst zodat medewerkers het daar vanaf kunnen halen en er zijn nog wat andere stukken tekst daaromheen neergezet om dit stukje bewustwording neer te zetten'.
Er wordt op meerdere manieren gecommuniceerd over deze procedures. Divisies mogen hierin zelf een keuze maken hoe ze informatie tot zich willen nemen.

De gekozen maatregelen worden regelmatig geëvalueerd
Incidenten worden wel geëvalueerd.

Het beleid wordt na evaluatie indien nodig aangepast
Vanuit meldingen kom je er soms achter dat er ergens iets niet klopt in het proces en als je dat oplost dan zie je dat het aantal meldingen terugloopt.

7.12 Analyse zorginstelling L

Actieve betrokkenheid van het bestuur

Oorspronkelijk kwam het idee om de functie van functionaris gegevensbescherming in te voeren van het Hoofd Bedrijfsvoering. Die heeft het bespreekbaar gemaakt bij de Raad van Bestuur.
De voorzitter van de Raad van Bestuur is portefeuillehouder van informatiebeveiliging. L: Het Hoofd bedrijfsondersteuning is gedelegeerd opdrachtnemer en mijn collega informatiemanager die is degene die het project leidt binnen de instelling en ik ondersteun daarbij. Ik zit in het stafbureau en mijn leidinggevende is het hoofd van het stafbureau en die valt onder Raad van Bestuur'.
Bij hoog risico incidenten moet er op Raad van Bestuursniveau worden besloten. Van alle meldingen worden rapportages gemaakt en die worden standaard in het MT besproken.
De Raad van Bestuur is dus actief betrokken bij informatiebeveiliging en privacy.

Prioriteit van privacy in organisatie
L geeft aan dat privacy niet de hoogste prioriteit heeft. L: 'Nou ik kan de Raad van Bestuur en het MT wel meekrijgen, maar als je naar de praktijk kijkt, de werkvloer dan is dat bijzonder lastig om zo'n taai thema ook ingevoerd te krijgen. Want waar zij zich op de werkvloer druk over maken is hun productie, de patiëntenzorg dat staat bij hen voorop. En dan komt informatiebeveiliging echt op een lager prioriteitsniveau te staan'.
L geeft aan dat informatiebeveiliging ook niet op de agenda's staat: 'Nee, sterker nog het veilig incidenten melden dat zou een vast agendapunt moeten zijn binnen teamoverleggen, maar daar komen ze niet aan toe joh. Ze zijn gewoon meer met de dagelijkse dingen op de werkvloer bezig dan met dat soort thema's.
L geeft aan dat het lastig is om aandacht te krijgen voor informatiebeveiligingsbeleid.

Er is een risico-inventarisatie gedaan
Zorginstelling L heeft een risicoanalyse uitgevoerd en gekeken waar hun grootste dreigingen liggen en hoe groot de kans is dat een bepaald risico voorkomt.
De grootste risico's van een datalek zitten voor zorginstelling L aan de zachte kant. L: Informatiebeveiliging heeft twee kanten een harde kant en een zachte kant. En de harde kant hebben wij vrij goed ingericht denk ik. We hebben een deel van onze IT ook geoutsourcet en daar ook allerlei afspraken gemaakt met de leverancier. Maar wat je ziet is je kunt je netwerk, je applicaties, wel goed beveiligen, maar als mensen zich daar niet aan houden bijvoorbeeld aan wachtwoorden, aan autorisaties, dan kom je ook niet ver. Die zachte kant dat is nog een risico wat ons betreft en dan kunnen het gewoon menselijke fouten zijn waardoor gegevens op de verkeerde plek terechtkomen of gegevens op de verkeerde plek worden opgeslagen of dat men zich gewoon niet bewust is van de afspraak dat je bijvoorbeeld niet je inloggegevens aan iemand anders mag afgeven, dus wat ons betreft is dat nu toch het grootste risico'.

Risico's van een beveiligingsissue zijn in beeld bij bestuur
Hoog risico incidenten worden besproken met de Raad van Bestuur en rapportages worden besproken in MT overleggen. Er zijn dus wel risico's in beeld bij Raad van Bestuur.

Er is op basis van risico-inventarisatie een beleidsdocument informatiebeveiliging opgesteld
De NEN-7510 is gebruikt als kader voor het opstellen van informatiebeveiligingsbeleid. L: 'De eerste stap die we vervolgens hebben gezet is beleid ontwikkelen. En wat we eigenlijk niet wilden doen is er een apart riedeltje voor ophangen, dus we wilden zoveel mogelijk aansluiten bij het kwaliteitsmanagementsysteem dat we hebben vanuit de HKZ. Dus informatiebeveiliging is daar gewoon een onderdeel van geworden en we hebben gekeken van nou oké wat is ons beleid ten aanzien van informatiebeveiliging. Hoe kijken wij er tegenaan? Wat vinden wij informatiebeveiliging? Wat vinden wij belangrijk? En van daaruit zijn we verder gaan kijken naar de inrichting. En dat is eigenlijk anderhalf jaar geleden dat we daarmee zijn begonnen'.
Er is nu in kaart gebracht wie verantwoordelijk is voor wat en daarnaast heeft zorginstelling L gekeken naar hun hele IT-landschap. L: 'Dus de hele organisatie om informatiebeveiliging heen dat is in kaart gebracht en beschreven'.
Er worden maatregelen genomen als mensen zich niet aan de gedragscode houden, die ook is opgesteld voor informatiebeveiliging.
Er is ook een nulmeting gedaan. L: 'Zij hebben eigenlijk geconstateerd dat we goed op weg zijn. Er waren een aantal aandachtspunten als het gaat om de toegang tot applicaties. Dan had ik een specifiek iets over authenticatie. En we moesten nog het een en ander doen op het gebied van die riscioanalyse dat mocht nog wat uitgebreider, dat hadden we vrij globaal en snel in elkaar gezet. Dsu dat was één van de aandachtspunten en we moesten nog wat beter met onze leveranciers afspraken maken en niet alleen onze leveranciers maar

ook onze financierders aan wie we gegevens verstrekken dat zij zich ook bewust zijn van de verantwoordelijkheid die zij hebben als wij gegevens uitwisselen. Dat zijn de belangrijkste punten geweest. En dat zijn allemaal punten die we nu hebben opgepakt en die risicoanalyse die hebben we nu gedaan en dat is af. En die awareness dat is eigenlijk de volgende stap die we nu willen gaan zetten'.

Er wordt regelmatig gecommuniceerd over het informatiebeveiligingsbeleid
Zorginstelling L is niet bekend met de 'ZEKER' campagne.
Er is geen specifiek communicatiebeleid op het gebied van informatiebeveiliging.
Alle documentatie op het gebied van informatiebeveiliging is gelinkt aan het kwaliteitsmanagementsysteem. Mensen kunnen hier de beleidsafspraken vinden. Ook heeft zorginstelling L een kwaliteitshandboek waar ook iets over informatiebeveiliging in staat.
De beleidsafspraken zijn wel te vinden, maar er wordt niet speciaal over gecommuniceerd.

Er wordt gewerkt aan het verhogen van beveiligingsbewustzijn in de organisatie
L geeft aan dat ze nu wel bezig zijn met kijken of het materiaal van een awarenesscampagne van de GGZ bruikbaar is voor hun instelling. Ook is door zorginstelling L zelf gekeken naar awareness. Er is een e-learning ontwikkeld, die mensen kunnen volgen, maar de campagne zelf moet zorginstelling L nog opstarten. In de e-learning komen onderwerpen als je computer uitloggen, autorisaties en wachtwoordbeleid voor.
Er zijn bij zorginstelling L nog geen ideeën over het opzetten van een campagne. L: 'Aan de ene kant wil je geen grote campagne opzetten, omdat het iets van de mensen zelf moet worden, dus het moet niet een apart iets worden. En wat ik net ook al zei: je moet het herkenbaar voor ze maken en als je het herkenbaar voor ze maakt dan slaat het vaak beter aan dan als je daar een hele campagne voor gaat opzetten. Dus daar zijn we nog even naar aan het zoeken van ja wat is wijsheid? Willen we daar echt bijeenkomsten voor organiseren waar ze allemaal naar toe moeten gaan? Dat daar presentaties en workshops over plaatsvinden. Of wil je dat in de bestaande overleggen en structuren en systeemn gaan uitrollen? Dus dat zijn vraagstukken waar we nog mee zitten'.
Zorinstelling L heeft een e-learning en is aan het kijken naar een awarenesscampagne er wordt dus gewerkt aan het verhogen van beveiligingsbewustzijn.

Er zijn duidelijke procedures aanwezig voor het behandelen van beveiligingsincidenten
Er is een procedure opgesteld voor het melden van incidenten. L: 'We hebben een a4 opgesteld van voorbeeld incidenten aan de hand van die vaste thema's: wachtwoordbeleid, autorisatie, phishing. Ook hebben we gezegd als je rare dingen tegenkomt meld het dan. We hebben een veilig-incidenten-melden-systeem en daar hebben we informatiebeveiliging een onderdeel van gemaakt. Dus als mensen bijvoorbeeld bij de printer een dossier met gegevens van de patiënten zien liggen dan moeten ze dat gaan melden. Dan komt dat bij mij, de informatiemanager en bij de manager van degene die het heeft gemeld en dan wordt dat geanalyseerd en dan kijken we van hee hoe komt het nou dat dat kan gebeuren? En zo proberen we dat wel langzaamaan bespreekbaar te maken'. Vervolgens wordt samen met de manager bepaald of het een hoog risico incident is en als dat zo is dan moet op Raad van Bestuursniveau een beslissing worden genomen.
Op het a4tje staat duidelijk beschreven welke incidenten je moet melden en ook wordt uitgelegd hoe er na een melding met de melding wordt omgegaan.

Er wordt regelmatig over deze procedures gecommuniceerd
Het opgestelde a4tje is via de lijn gecommuniceerd. L: 'We communiceren altijd beleidsafspraken via de directie. De directie communiceert dat naar de managers en de managers moeten dat met hun team bespreken. 'Dat gaat in vaste overleggen. We hebben een overlegstructuur. Eén keer in de maand hebben we bijvoorbeeld het MT, daarna hebben we de eigen RVEs (Resultaat Verantwoordelijke Eenheden). We hebben drie RVEs dan wordt het in het MT van de RVE's besproken en daar zitten alle managers bij en die horen dat met hun eigen teams te bespreken in hun eigen werkoverleg'.
Ook heeft zorginstelling L een intranet waar regelmatig berichten worden geplaatst, maar L geeft aan dat niet iedereen intranet leest, dus dat je dan echt een minimum aan medewerkers bereikt die dat gaan lezen.
Zorginstelling L heeft nog geen posters. L: 'Het enige wat we tot nu toe hebben gedaan is de berichten op intranet. We houden een FAQ bij en that's it. Voor de rest hebben we er geen grote communicatiecampagne aan gehangen'. Er wordt dus wel af en toe gecommuniceerd, maar niet regelmatig.

De gekozen maatregelen worden regelmatig geëvalueerd
De rapportages worden besproken in het MT en dan wordt gekeken naar de bevindingen van hee wat zien we nou? De trend wordt besproken en dan ook eventueel de maatregelen die daarop genomen moeten worden.

Het beleid wordt na evaluatie indien nodig aangepast

Bijlage 8 Samenvatting analyse per instelling

Zorginstelling A (UMC)
Het bestuur van zorginstelling A is wel betrokken bij het privacythema, maar niet heel actief. De privacycommissie regelt zaken over het algemeen. Privacy heeft wel prioriteit in zorginstelling A. Er is bijvoorbeeld een privacycommissie in het leven geroepen en er is een bestuurslid portefeuillehouder van privacy. Toch verschilt het volgens A wel per persoon hoeveel belang men hecht aan privacy. Ook is er een beleidsdocument informatiebeveiliging aanwezig en zijn de risico's in kaart gebracht. Het beleidsdocument wordt regelmatig gecommuniceerd en er wordt gewerkt aan beveiligingsbewustzijn in zorginstelling A. Ook zijn er duidelijke procedures aanwezig voor het behandelen van beveiligingsincidenten en wordt er regelmatig over die procedures gecommuniceerd.

Zorginstelling B (ZIEKENHUIS)
Het bestuur van zorginstelling B is actief betrokken bij het privacythema. Er is maandelijks overleg met de Raad van Bestuur en de Raad van Bestuur is ook hoofdelijk aansprakelijk als het misgaat. Er lijkt daarentegen geen prioriteit te zijn voor privacy in de organisatie. Het bestuur geeft niet aan of er aandacht gegeven moet worden aan privacy. Er is ook enkel aandacht voor het risico op boetes en niet voor het vertrouwenverlies van patiënten of reputatieschade. Zorginstelling B beschikt over een beleidsdocument informatiebeveiliging en hierover wordt regelmatig gecommuniceerd. Er wordt nog niet actief gewerkt aan het verhogen van beveiligingsbewustzijn in zorginstelling B. Wel zijn er duidelijke procedures voor datalekken aanwezig en wordt er op verschillende manieren over deze procedures gecommuniceerd.

Zorginstelling C (kleinere zorginstelling/thuiszorg)
Het bestuur van zorginstelling C is actief betrokken bij het privacythema en privacy heeft ook prioriteit in de organisatie. Er is een beleidsdocument informatiebeveiliging en hierover wordt regelmatig gecommuniceerd. Ook wordt er gewerkt aan het verhogen van beveiligingsbewustzijn. De procedure rondom beveiligingsincidenten kan duidelijker in zorginstelling C. Er wordt wel regelmatig over de procedures gecommuniceerd.

Zorginstelling D (kleinere zorginstelling/GGZ)
Dankzij maandelijkse overleggen is het bestuur actief betrokken bij het informatiebeveiligingsbeleid. Ook is er prioriteit voor privacy volgens D. Er worden hier echter geen duidelijke argumenten voor aangedragen. De imagoschade ziet D als grootste risico. De menselijke factor is de grootste kwetsbaarheid. Bij het bestuur zijn de boetes als risico in beeld. Er wordt nog niet regelmatig gecommuniceerd over het informatiebeveiligingsbeleid en er wordt ook nog niet actief gewerkt aan het verhogen van beveiligingsbewustzijn in de organisatie. Er zijn ook nog geen duidelijk beschreven specifieke procedures. D geeft aan dat er in het verleden al campagnes geweest zijn voor het incident-meldsysteem en dat het daarom niet nodig is om medewerkers hier opnieuw in te trainen.

Zorginstelling E (kleinere zorginstelling/GGZ)
Het bestuur van zorginstelling E is actief betrokken bij het informatiebeveiligingsbeleid en privacy heeft prioriteit in zorginstelling E. De risico's op een boete zijn in beeld bij het bestuur en er is een plan van aanpak geschreven voor de komende twee jaar. Datalekken wordt als eerste thema aangepakt in de communicatie, maar dit moet nog tot uitvoering worden gebracht. Er zijn al wel ideeën over het werken aan beveiligingsbewustzijn maar er wordt nog niet actief aan gewerkt. Er is al wel een protocol datalekken opgesteld en hierover wordt ook regelmatig gecommuniceerd.

Zorginstelling F (Ziekenhuis)
Het bestuur van zorginstelling F is wel betrokken bij privacy, maar niet actief. Zorginstelling F is al lang bezig met privacy en het is ieder jaar een terugkerend thema. Voor zorginstelling F is het belangrijkste dat patiënten erop moeten kunnen vertrouwen dat hun gegevens bij zorginstelling F in goede handen zijn. De Raad van Bestuur wordt bovendien wakker als het gaat om de boetes. Er wordt op veel verschillende manieren gecommuniceerd over het informatiebeveiligingsbeleid en er wordt ook gewerkt aan het verhogen van beveiligingsbewustzijn met behulp van bewustwordingscampagnes. Ook is er duidelijk hoe je een datalek moet

melden bij zorginstelling F. De procedure zou alleen nog wel wat duidelijker en meer gespecificeerd mogen. Over de procedure wordt regelmatig gecommuniceerd.

Zorginstelling G (kleinere zorginstelling/vvt)
Er is bij zorginstelling G formeel nog niet echt commitment van het management, maar er wordt wel altijd overlegt met het bestuur voor er iets gebeurt. G heeft ook regelmatig overleg met de Raad van Bestuur. Volgens G krijgt privacy wel de juiste prioriteit. Er wordt op verschillende manieren gecommuniceerd over het informatiebeveiligingsbeleid en er wordt gewerkt aan awareness met behulp van een awarenesstraining die verplicht is voor iedereen om te volgen. Ook is er een intern meldpunt voor datalekken, maar deze is nog niet in het systeem geïntegreerd. Er wordt wel regelmatig over de procedures gecommuniceerd.

Zorginstelling H (UMC)
Het bestuur in zorginstelling H is actief betrokken bij het privacybeleid. Er is ook een hoge prioriteit van privacy in de organisatie mede dankzij een incident van een paar jaar terug. Het grootste risico is volgens zorginstelling H het gebrek aan awareness. Voor de organisatie is dit reputatieschade. Deze risico's zijn ook in beeld bij de Raad van Bestuur. Er is een vast persoon bij de communicatieafdeling waarmee de communicatie wordt afgestemd. Er wordt regelmatig gecommuniceerd over het informatiebeveiligingsbeleid. Het communiceren van de procedures is niet ter sprake gekomen. Wel wordt er gewerkt aan het verhogen van beveiligingsbewustzijn. Ook zijn er hele duidelijke procedures opgesteld voor datalekken.

Zorginstelling I (kleinere zorginstelling/)
Het bestuur van zorginstelling I is niet betrokken bij het beleid. Alle plannen liggen ter goedkeuring bij de Raad van Bestuur, maar deze doet hier niets mee. Ook zijn de risico's niet echt goed in beeld bij de Raad van Bestuur. Er zijn wel duidelijke plannen opgesteld door I voor de komende twee jaar, maar deze moeten allemaal nog uitgevoerd worden.

Zorginstelling J (Ziekenhuis)
Het bestuur van zorginstelling J is actief betrokken bij het beleid en vindt het ook belangrijk om een gemeenschappelijke betrokkenheid te hebben, omdat het onderwerp alle bedrijfsonderdelen van je organisatie raakt. Ook is er prioriteit voor privacy in zorginstelling J. Teammanagers geven soms wel aan het onderwerp onzin te vinden. De risico's zijn goed in beeld bij de Raad van Bestuur. Er wordt op verschillende manieren gecommuniceerd over het informatiebeveiligingsbeleid en er wordt gewerkt aan het verhogen van bewustzijn met behulp van een e-learning en voorlichting. Er wordt duidelijk welke manier van melden zorginstelling J hanteert, maar de procedures zouden wat duidelijker mogen worden omschreven. Wel wordt er op verschillende manieren gecommuniceerd over de procedures.

Zorginstelling K (UMC)
Het bestuur van zorginstelling K is niet actief betrokken bij het privacybeleid. Privacy heeft wel een hoge prioriteit in zorginstelling K, het staat zelfs in de top 5 van de Raad van Bestuur. Er wordt niet duidelijk of de risico's in beeld zijn bij het bestuur, omdat K voornamelijk over technische risico's spreekt en niet over organisatorische risico's. Er wordt ook niet heel uitgebreid gecommuniceerd over het informatiebeveiligingsbeleid en er moet nog gewerkt worden aan het verhogen van beveiligingsbewustzijn. Hier zijn al wel plannen voor door een e-learningmodule te ontwerpen. Er wordt wel regelmatig over de procedures voor datalekken gecommuniceerd. De procedures zijn ook duidelijk en het proces na het doen van de melding ook.

Zorginstelling L (Kleinere zorginstelling/GGZ)
Het bestuur van zorginstelling L is actief betrokken bij privacy. L geeft aan dat privacy niet de hoogste prioriteit heeft in zorginstelling L het staat bijvoorbeeld niet op de agenda's en het is lastig om er aandacht voor te krijgen. Zorginstelling L heeft een uitgebreide risicoanalyse uitgevoerd en de hoog risico incidenten worden ook besproken met de Raad van Bestuur. Er is geen speciaal communicatiebeleid om te communiceren over informatiebeveiliging. Er wordt wel gewerkt aan het verhogen van beveiligingsbewustzijn met behulp van een e-learning en in de toekomst een awarenesscampagne. Er is een duidelijke procedure voor melden van

datalekken en dit is ook gecommuniceerd. Er wordt alleen niet regelmatig aandacht aan besteed. Enkel een bericht op intranet en een FAQ.