Information security in Dutch hospitals

Geert Wirken

Master thesis Content and Knowledge Engineering
Faculty of Science
Utrecht University
January 2012

Thesis number: IKU-3116239

First supervisor: dr. F. Wiering
Second supervisor: dr. M.R. Spruit

Table of contents

1. Summary

This thesis researches how Dutch hospitals improve information security. Information security has become an important topic for many Dutch hospitals, as they are since a few years required to comply with information security regulations. However, hospitals face various difficulties when improving information security and earlier research has shown that many hospitals did not comply with information security standards. Common practice in hospitals sometimes conflicts with information security measures: timely and unrestricted access to critical medical information is essential for effective treatment of patients, but on the other hand, medical information is often confidential and sensitive information which should not be disclosed to unauthorized persons. Furthermore, it is important that information systems are reliable and that the integrity of information is ensured.

This study aims to find out which problems Dutch hospitals face when improving information security, and how hospitals mitigate these problems. The conflicts of interest described above are important causes, but there are also other problems which prevents hospitals from complying to information security standards.

The research is divided in two phases. The first phase consists of a case study in one hospital, where problems with improving information security are analyzed in a detailed method. The second phase of the study is a validation study where the results of the case study are validated among a representative set of hospitals.

Various problems have been found by this study, but also many best practices have been found. These best practices are useful for other hospitals: they provide workable solutions that address both information security requirements, as well as medical requirements.

The main conclusions of this study are that hospitals should address information security seriously, and that hospitals should solve problems together when possible.

1.1 Nederlandse samenvatting (Dutch summary)

Deze master thesis onderzoekt hoe Nederlandse ziekenhuizen informatiebeveiliging verbeteren. Informatiebeveiliging is voor Nederlandse ziekenhuizen een belangrijk onderwerp geworden: sinds een aantal jaar moeten ziekenhuizen wettelijk voldoen aan beveiligingseisen en –standaarden. Dit is echter problematisch voor veel ziekenhuizen: eerder onderzoek heeft aangetoond dat veel ziekenhuizen problemen hebben met het verbeteren van informatiebeveiliging en veel ziekenhuizen voldeden niet aan de vereiste standaarden. De praktijk in ziekenhuizen levert soms conflicten op met beveiligingseisen: tijdige en onbeperkte toegang tot belangrijke medische informatie is soms essentieel voor effectieve patiëntenzorg, maar toegang tot medische informatie moet aan de andere kant beperkt worden tot geautoriseerde medewerkers – medische informatie is vaak vertrouwelijke en gevoelige informatie. Verder is het belangrijk dat informatiesystemen betrouwbaar zijn en dat integriteit van informatie gewaarborgd is.

Dit onderzoek probeert te achterhalen welke problemen Nederlandse ziekenhuizen hebben met het verbeteren van informatiebeveiliging, en hoe ziekenhuizen deze problemen oplossen. De hierboven beschreven belangenconflicten zijn belangrijke oorzaken, maar er zijn ook andere problemen die ertoe leiden dat ziekenhuizen niet voldoen aan beveiligingseisen.

Het onderzoek is verdeeld in twee fases. De eerste fase bestaat uit een casestudy in een ziekenhuis, waar de problemen met het verbeteren van informatiebeveiliging gedetailleerd worden onderzocht. De tweede fase bestaat uit een validerend onderzoek, waarbij de resultaten uit de casestudy worden getoetst onder een representatieve groep ziekenhuizen.

Er zijn verschillende problemen gevonden in dit onderzoek, maar er zijn ook een aantal ‘best practices’ gevonden: oplossingen voor problemen die door sommige ziekenhuizen succesvol worden gebruikt. Deze best practices zijn nuttig voor andere ziekenhuizen, het zijn werkbare oplossingen die zowel aan informatiebeveiligingseisen als aan medische eisen recht doen.

De belangrijkste conclusies van dit onderzoek zijn dat ziekenhuizen informatiebeveiliging op een serieuze manier moeten benaderen om te kunnen voldoen aan de geldende richtlijnen, en dat problemen gezamenlijk opgelost moeten worden.

2. Introduction

Hospitals are organizations which typically process a lot of information daily. Think for instance of the medical information of patients: a typical hospital is visited by thousands of patients each year and for each patient, the hospital needs to store contact details, insurance information, appointments with medical specialists, and a medical data: medical reports, radiography pictures, laboratory results and more.

All this information is processed by various persons within an hospital organization. Medical professionals need to access medical information for effective treatment of a patient; administrative departments need to know which medical operations have been performed to receive reimbursement, et cetera.

The amount of information that hospitals process and the nature of this information make it important that hospitals handle this information with care. Medical information is sensitive information, and hospitals should ensure that this information is processes carefully.

However, Dutch hospitals face a variety of new developments since the past decade, and these developments influence the way hospitals process information. In general, the following developments are observed:

- There is an increasing focus on costs and quality of healthcare provided by hospitals;
- Information technology is increasingly used by Dutch hospitals;
- Citizens are becoming more aware of privacy issues, resulting in security requirements for hospitals;
- Hospitals have certain unique aspects which makes it sometimes difficult to establish effective information security.

These developments are further discussed in the following sections and are further discussed in chapter 4. They are introduced here already because they are important to define the research problem. This chapter ends with a reading guide.

2.1 Greater focus on costs and quality

In 2006, the Dutch health care system was reformed significantly. The main idea behind this reform was that hospitals should operate more efficiently, bringing less costs. Furthermore, the idea was that market mechanisms would play a bigger role: hospitals would be in a competition with other hospitals and independent specialists. This would reduce costs further and also contribute to a greater transparency in health costs. Non-profit healthcare insurers were also privatized as part of this reform and it was made easier for patients to switch between healthcare insurers. The idea behind this reform was that there would be more competition between healthcare insurers, with a larger focus on healthcare costs and quality. The reform introduced the possibility for insurers to discontinue reimbursement for certain medical treatments in every hospital (for example, treatments in expensive hospitals are not reimbursed) which made it more important for hospitals to advertise themselves and to make themselves appealing to patients and healthcare insurers.

As part of this development, there is a greater focus on costs, healthcare quality and transparency. Hospitals have to remain competitive while maintaining good quality of the healthcare provided.

2.2 Increasing usage of information technology

Another development is the increasing usage of information technology in the healthcare sector. Almost every hospital uses an hospital information system to schedule appointments,

for financial administration and other purposes. Information technology is also employed to support medical processes: radiology pictures are for instance processed via electronic information systems and pharmacy orders are processed and verified electronically. Many hospitals are transforming to a system where all patient information is processed electronically, in order to increase efficiency and to make information better available.

Another example of the increasing usage of information technology by Dutch hospitals is the introduction of a country-wide system to exchange medical information between healthcare providers electronically, the so called 'elektronisch patiëntendossier' (electronic patient record). This system enables healthcare professionals to access medical information of every Dutch citizen electronically, reducing the time to retrieve medical information, increasing the availability of it and improving the readability and exchangeability of medical information.

2.3 Increasing awareness of privacy issues

While the processing of patient data via electronic systems provide great benefits to both patients and healthcare providers, patients have also become aware of the sensitiveness of medical records and have been concerned about their privacy in a system where medical information is exchanged electronically. The introduction of a national electronic patient record has been significantly delayed due to privacy concerns and a proposed law to make this system obligatory has eventually been voted down by the Dutch senate, mainly because of privacy concerns.

Medical data is information that is potentially very sensitive and very personal. It can also have a severe impact on one's life: employers could refuse a contract if he or she knows that an employee suffers from psychological problems. Healthcare insurers could reject to insure a person if s/he has a serious, life-threatening disease (or they could raise the premium). And then there are personal circumstances where it is not desirable that a person's relatives, colleagues or friends know about the medical state of someone. Hospitals process large amounts of medical information and because of the nature of this information, they should be very careful in handling it: unauthorized disclosure of medical information is not acceptable. Therefore, hospitals should take security measures to prevent such disclosures and to maintain privacy for their patients.

Privacy plays also a role in the trust that patients have in the healthcare system. When patients suspect that an hospital disrespects the patient's privacy, the patient could be less willing to provide vital medical information. Besides the trust aspect and ethical aspects, there is also a legal issue: doctors are pledged to secrecy and they cannot share medical information without justification. This also implies that medical professionals should take care to protect medical information of their patients.

The Dutch healthcare sector has established a standard for securing information in hospitals and other healthcare organizations, the NEN 7510 standard. This standard defines various security requirements for healthcare organizations, such as minimum requirements for passwords and access to electronic information systems. The Dutch government made compliance to this standard mandatory by introducing a law in 2008[1] by referring to this standard.

[1] Regeling gebruik burgerservicenummer in de zorg, 2008, art. 2

2.4 Unique security aspects of the healthcare industry

There are currently various generic standards on information security. However, standard approaches to secure information which are sufficient for typical organizations cannot always be applied to the healthcare sector: in some aspects, healthcare organizations are different from other organizations.

Medical information is potentially very sensitive and should not be accessible to persons who have no need or authorization for that information. As described before, privacy plays a large role in medical information. Therefore, it would make sense to protect this information very strictly. However, providing effective healthcare depends for a large part on communication between various medical professionals and an effective exchange of information. Furthermore, this information sometimes needs to be accessed very quickly – imagine for instance an emergency room in an hospital, where urgent treatment is necessary and delay in communication could have a negative impact on the patient's health. Waiting for authorization or restricting access to this information in non-public parts of the hospital would have severe drawbacks in terms of patient safety. This outlines a contradiction: medical data is very sensitive and should be protected likewise, but quick access to information is sometimes necessary for effective patient treatment. Which is more important?

Another aspect which distinguishes healthcare organizations from other organizations is that it depends on the integrity and completeness of the information. Missing, outdated or wrong information can be life-threatening and actions based on such false information can have severe consequences. Medical information should always be available – office workers can wait a few hours if the network goes down, but doctors in the operating room cannot.

Furthermore, hospitals are often large and public buildings, with only few restrictions to enter certain areas. There are many professionals, patients and visitors and the physical security is difficult to establish –social surveillance is difficult because of the size of the organization and visitors can access many parts of the hospital building with valid reasons. This problem is not unique to the healthcare sector, but it is an aspect which typically plays a role in (large) hospitals. This implies that it is even harder to secure patient information, because physical access is relatively easy.

All these reasons indicate that hospitals are more complex, more demanding and more difficult to secure than other organizations of comparable size. Hospitals are forced to comply with security regulations by law, but compliance would sometimes require drastic changes to the organization or processes.

2.5 Motivation

All in all, there are various important developments that can be seen. Hospitals are subject to increased market forces and have to operate competitively. For efficiency reasons, hospitals increasingly process and exchange information via electronic information systems. However, patients have become concerned about their privacy rights, which requires hospitals to take security measures to protect privacy for patients and to secure access to sensitive information. There are standards for protecting this information, but hospitals face difficulties with implementing these standards because of the specific demands within the healthcare sector.

In 2008, the Dutch Health Care Inspectorate (Inspectie voor de Gezondheidszorg) and the Dutch Data Protection Authority (College Bescherming Persoonsgegevens) visited various hospitals throughout the Netherlands and investigated to what extent these hospitals complied to the NEN 7510 regulations. The authorities found that almost all hospitals were not compliant and only adhered partly to the standard. Furthermore, in many hospitals, there was

no clear vision how the hospital should enforce privacy and data security and many aspects were settled in practice by the IT department.

This raises the question why so many hospitals did not implement sufficient security measures to comply with the standard, considering the developments outline above: patients demand that their privacy is respected and that measures are taken against unauthorized disclosure of medical information, especially when an increasing amount of information is processed and exchanged via electronic information systems. Besides that, implementing security measures is required by law.

This study aims to find out how Dutch hospitals address this problem and what obstacles are encountered while improving information security.

2.6 Reading guide

The next chapter (chapter 3) defines the research problems more specifically.

In chapter 4, related literature and earlier research will be presented. Some elements that are discussed in this introduction are further elaborated by providing related literature on information security, on information security standards, and on the Dutch healthcare system. Earlier research on information security in Dutch hospitals is also presented. This chapter provides more insights in the domains that are being researched.

Chapter 5 defines the hypotheses and discusses the general research approach. The hypotheses are defined in this chapter, based on the research questions defined in chapter 3 and the additional insights presented in chapter 4. The research approach that is presented in this chapter is the general, high-level research approach.

In chapter 6 and chapter 7, the results of the actual research are provided. The research itself consists of two phases; each phase is presented in a separate chapter. Each chapter starts with a description of the research method used for that phase and is followed by the presentation of the results. Chapter 6 describes the first phase (a case study at one hospital), chapter 7 describes the second phase (a validation study at multiple hospitals).

The results of both phases are analyzed in chapter 8. Differences and resemblances between the first and the second phase within this study are discussed.

Chapter 9 presents the conclusions and answers the research questions posed in chapter 3. This chapter also presents some recommendations for future research.

3. Research problem

The introduction gave an overview of current developments in the Dutch hospital sector. Some of the described developments (introduction of market forces, increased influence of healthcare insurers) have led to a stronger focus on costs and efficiency. Another important development is the increasing usage of information technology in the hospital sector, which means that more and more information is processed and exchanged via electronic information systems. While this has improved efficiency and the availability of medical information, the usage of these systems have also raised privacy and security issues, as already described in the previous chapter.

Medical data is very sensitive and needs to be protected against malicious usage. However, on the other hand, it is very important that medical information is available as timely as possible for medical workers, to improve the quality of care provided to a patient and to choose a treatment based on all available information. Both the security and privacy aspects related to this information need to be addressed. On top of this, hospitals are required to comply with certain security standards and data protection laws.

The above leads to the observation that hospitals face a certain need for effective information security. On one hand, they are legally obliged to take security measures and protect medical information – hospitals would risk legal action if they do not take enough security measures. Furthermore, the fact that more and more information is processed electronically means that the consequences of security breaches are also larger: more information is exposed to security risks. Another important driver for the need of effective information security is the possibility of negative publicity in case of a security breach.

However, there are other factors that impact the need for information security. As said, hospitals are subject to cost reductions and competition, which means that information security should be cost-effective. Another factor is the specific environment of hospitals: it is reasonable to expect that some security requirements conflict with other interests within the hospital.

Earlier research has already showed that Dutch hospitals have difficulty complying to the industry's security standards (College Bescherming Persoonsgegevens & Inspectie voor de Gezondheidszorg, 2008) and this raises the question why hospitals do not comply with the security standards. Some reasons have been provided above, but are there other reasons why hospitals do not fully comply with security standards? What is the best way to improve information security, and how can hospitals comply with information standards?

Based on the above questions, it is possible to derive the following main research question:

> *How can hospitals improve information security successfully and in compliance with mandatory standards?*

This question includes both how information security can be improved successfully and how hospitals can comply with security standards. The question faces various aspects. For instance, it is important to know how hospitals in the Netherlands are currently improving information security – is the approach common or are there various approaches? Besides the actual approach that hospitals adhere, information about problems with improving information security are important. It is reasonable to assume that there are problems that are common for many Dutch hospitals: to a certain extent, the hospitals are comparable to each other.

It is important to note that the main research question contains no reference to the term 'privacy'. Information security encompasses three important objectives: confidentiality,

integrity and availability. The next chapter will elaborate on these concepts, for now it is important to realize that privacy is only one aspect of information security (besides others) and that the confidentiality aspect covers most of the privacy issues.

While many hospitals may struggle with a certain security problem, it is also possible that one hospital has found an efficient solution to this problem (e.g., by modifying a procedure) – maybe it is even possible to find a 'design pattern' or 'best practice', a certain approach that is used by a large amount of organizations. Gathering examples of such successful practices is useful for other hospitals.

Taking all this into account, it is possible to define the following four sub questions:

1. How do hospitals currently implement security regulations?
2. Do hospitals encounter problems while improving information security? If so, what are these problems?
3. Is it possible to distinguish a common pattern or 'best practices'?
4. How do hospitals comply with the standards?

This study takes an explorative approach. Based on earlier research, it is known that there are difficulties in improving information security, and this study aims to find out what these problems are. On the other hand, it can be expected that there are hospitals which have taken an efficient set of security measures or which have found an effective approach to improve information security. Insight in the process of implementing information security in Dutch hospitals, by both analyzing problems and successful approaches, will gain more insight into the complexity of this subject and specific demands and problems in this sector. The results of this study will be useful to at least Dutch hospitals, which may learn from approaches adhered by other hospitals, but the results of this study are presumably also useful for hospitals in other countries. The specific regulations and requirements may vary from country to country, but the main problem of addressing information security is comparable.

The following diagram presents the observed developments, consequences and resulting research questions in a more structured way. First, the developments that have been described in the introduction are listed, and the consequences of these developments. As described above, these consequences lead to a certain need for effective information security. This in turn results in a main research question and four (abbreviated) sub questions.

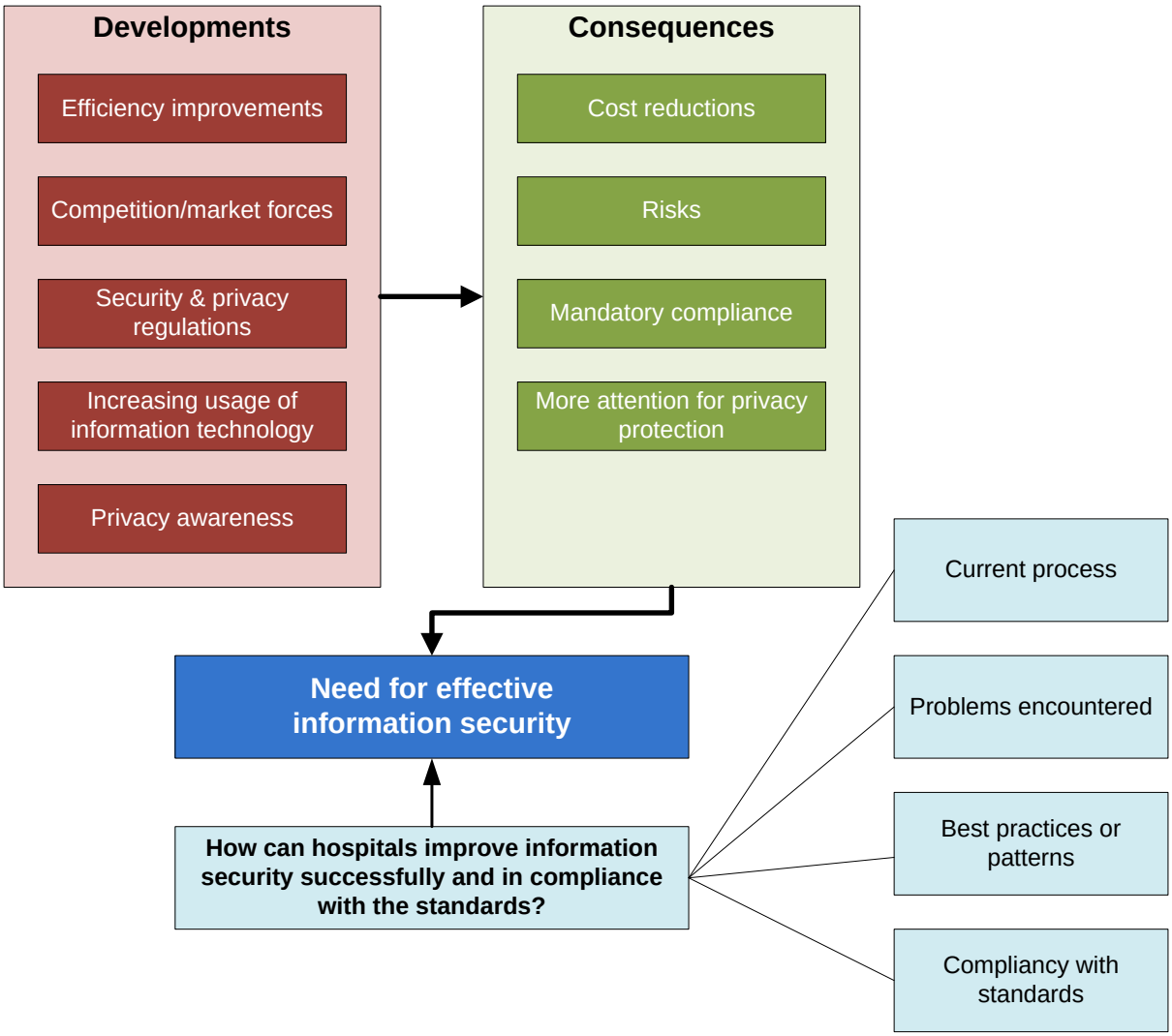


Figure 3.1: Diagram of the research problem.

The following chapter (chapter 4) will discuss related literature and earlier research on information security in Dutch hospitals. Chapter 5 describes the research approach and the hypotheses that are tested. Chapter 6 and further describe the research and the results of it.

4. Theory and related literature

This section describes the theoretical framework behind the research and related studies. First, some general literature on information security will be discussed, including international and national standards for information security. After that, the organization of the Dutch healthcare system is described. This chapter ends with a discussion on the current state of information security in Dutch hospitals, including earlier research on this subject.

4.1 Information security

Information security is the field of study which concentrates itself on the protection of information. Protection of information is important to organizations, because information can be valuable to them and others. Unauthorized disclosure of information can have severe consequences for an organization. Besides preventing unauthorized disclosure, it is also important to prevent loss of information. A bank, for instance, would suffer severe losses if the account balances are lost.

This section describes important concepts in information security (which have been mentioned briefly in the previous chapter) and it lists some definitions for information security.

4.1.1 What is information security?

There are various definitions on information security. Peltier (2001) states that "information security encompasses the use of physical and logical data access controls to ensure the proper use of data and to prohibit unauthorized or accidental modification, destruction, disclosure, loss or access to automated or manual records and files as well as loss, damage or misuse of information assets". Pfleeger and Pfleeger (2003) define information security as follows: "Computer security attempts to ensure the confidentiality, integrity and availability of computing systems' components".

Anderson (2003) opposes to the definitions above, because these definitions are very broad and they also describe activities that are not part of information security. However, it is important to have a precise definition. Anderson proposes the following definition: *"A well-informed sense of assurance that information risks and controls are in balance"*.

This definition gives attention to the aspect of assurance: information security measures are being taken to have a certain level of assurance against security risks. Organizations should have the confidence that their information is protected. Another aspect of this definition is the balance between risks and controls: certain security measures (controls) have to be taken to mitigate risks, but controls needs to be weighed against risks. Anderson (2003) remarks that often the consequence of information security risks are quite severe and will cost an organization more than the investment in effective controls, but it is exactly this type of balancing that needs to be done by an organization. Factors that also play a role in deciding on which security measures to take and to what extent are regulatory compliance, industry standards, and data about competitors. Another important aspect is cost effectiveness: implementing effective, inexpensive measures are usually favored over ineffective and costly security measures. All these aspects play a role in answering the question "How secure can we afford to be – or need to be?" (Anderson, 2003).

4.1.2 Important concepts in information security

Avizienis, Laprie, Randell and Landwehr (2004) define information security as a composite of the concepts *confidentiality*, *integrity* and *availability*. These three concepts are important

concepts in the information security domain, and these concepts are sometimes referred to as the 'CIA triad' (Yskout, Heyman, Scandariato and Joosen, 2008). The concepts can be seen as objectives for information security.

Avizienis et al. (2004) define confidentiality, integrity and availability as follows:

- **Confidentiality**
  The absence of unauthorized disclosure of information.
  This implies that disclosure of information should be restricted. It should be clearly defined which entities (persons, organizations) have access to information. Measures should be taken to prevent disclosure to unauthorized entities.
- **Integrity**
  The absence of improper system alterations.
  This concept implies that information should not be altered improperly: data should not be corrupted (e.g. a database corruption) or deleted accidentally. This aspect also implies that information that is inserted, modified or deleted should be correct; this aspect is not necessarily limited to technical integrity of information.
- **Availability**
  The readiness for correct service.
  This concept says that information systems should be available for service when needed. The term 'correct service' implies that the system should be in a state where it functions as expected; when an information system does not perform as expected (e.g. the functionality is limited, or information is not accessible due to maintenance), it is considered to be unavailable.

These three aspects describe the most important elements of information security: disclosing correct information (integrity) to only authorized entities (confidentiality) when requested (availability). However, some authors have identified additional concepts to the CIA triad. Yskout et al. (2008) recognize two additional aspects:

- **Accountability**
  The ability to hold users accountable for their actions.
  This aspect implies that actions within a system can be traced back to one unique entity, i.e., actions should be logged. It requires that entities cannot be impersonated, and that logs are subject to non-repudiation.
- **Privacy**
  The ability of an individual or group to control the flow of information about themselves.
  This aspect (sometimes referred to as 'anonymity') implies that organizations should provide means to individuals (or groups) to request which information is known about them and how this information is processed. Furthermore, a possibility should be provided to control this information or the flow of information, e.g. by removing or modifying information.

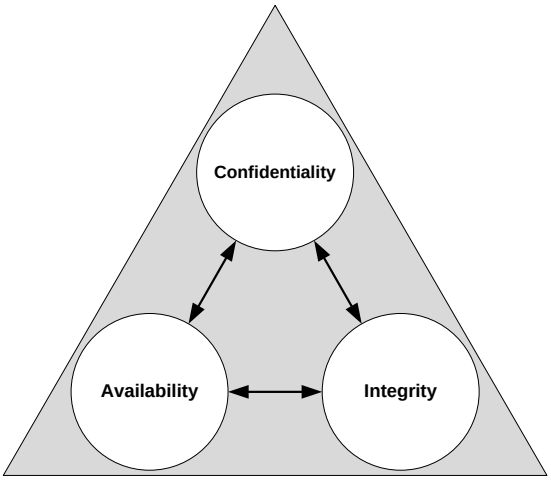


Figure 4.1: Graphical representation of the CIA triad.

As can be seen in Figure 4.1, the three aspects of the CIA triad are presented as opposites. This is because there is no reason to assume that all three aspects align seamlessly with each other. For instance, confidentiality of information and availability of information may conflict with each other: protecting information (to address the confidentiality aspect) harms the availability and accessibility of information.

4.1.3 Information security within organizations

Many organizations have to deal with information security: industries have to protect their trade secrets, banks have to protect financial data of their customers, hospitals have to protect medical information of their patients, and so on. There are various ways how organizations accomplish information security, but a common approach is creating a separate role for an information security officer who is dedicated to the subject of information security. The security officers plays an important role in improving information security: he or she usually makes an integral risk analysis, decides which security measures have to be taken and s/he raises awareness among employees.

4.2 Introduction to information security standards

There are various standards for information security, both international standards and national standards. Some are specifically aimed at medical informatics, others are generic standards that apply to various organization types. The following section gives a brief introduction to the various standards for information security that are relevant for this study.

To aid the reader, the following table is provided. It lists all standards that are discussed in this section.

Standard nr.[2]	**Description**[3]	**Remarks**
ISO 27000:2009	Overview of the ISO 27000 standards family.	Int. standard
ISO 27001:2005 *ISO 17799:2005*	Describes the requirements for an Information Security Management System (ISMS).	Int. standard

[2] ~~Strikethrough~~ standard numbers indicate that this version of the standard has been superseded by a revision or by another standard.

[3] For the ISO standards, this description is derived from the standard itself. The descriptions of the listed NEN standards have been provided by the author.

Standard nr.[2]	Description[3]	Remarks
ISO 27002:2005	Code of practice for information security management; provides widely accepted security controls.	Int. standard
ISO 27799:2008	ISMS guidance specifically aimed at the healthcare sector, based on ISO 27002.	Int. standard
~~NEN 7510:2004~~	Dutch standard, specifically aimed at the healthcare sector; based on ISO 17799:2000. *(Standard is superseded by NEN 7510:2011)*	Dutch standard, withdrawn
NEN 7510:2011	Revision on the 2004 version of NEN 7510; based on ISO 27799:2008.	Dutch standard
~~NEN 7511:2005~~	Specification of NEN 7510 for various types of healthcare organizations. *(Standard is superseded by NEN 7510:2011)*	Dutch standard, withdrawn
NEN 7512:2005	Dutch standard for secure exchange of healthcare information.	Dutch standard

Figure 4.2: List of relevant standards for information security.

4.2.1 International standards (ISO)

The International Organization for Standardization (ISO) has defined a family of more than ten standards about information security. These standards all deal with a separate part of information security: one standard describes for instance the requirements for an information security management system; another standard describes good information security practices, etc.

All ISO standards for information security are numbered in the range 27000 – 27999, which is why the collection of standards is sometimes called the ISO 27000 family or ISO 27k family.

Standards are distinguished by a standard number. The year in which a standard has been accepted is often added to the number. For instance, ISO 27001:2009 refers to the 2009 edition of ISO standard 27001. Standards are revised periodically, which explains the need to add the publication year when referring to a specific norm.

The ISO 27000 family is an extensive collection of standards. Important generic standards are ISO 27001 (information security management system) and ISO 27002 (best practices). For the healthcare sector, ISO 27799 is an important standard: this standard describes how ISO 27002 should be applied to healthcare organizations. The following sections discuss each standard shortly.

4.2.1.1 ISO 27000 – Information security management systems – Overview and vocabulary

ISO 27000 describes all standards that are part of the ISO 27000 family. Definitions that are used throughout all standards that are part of the ISO 27000 collection are defined in this standard. Some general concepts that are shared among these standards are also introduced in this standard. Furthermore, this standard argues why the presence of an information security management system is important.

4.2.1.2 ISO 27001 – Information security management system – requirements

This standard describes the requirements for an information security management system (ISMS). An ISMS is the whole set of policies, procedures, responsibilities, organizational structures and other aspects which are needed to establish, maintain and improve information security. In other words, an ISMS is the organizational system which enables security measures to be taken and evaluated within an organization. An important part of an ISMS is that measures are taken based on a business risk approach, so that effective measures can be taken (based on the risk analysis).

The standard describes the Plan-Do-Check-Act model: a cycle of four phases where the ISMS is established (plan); the policy, processes and procedures are implemented and executed (do); the results of the policy are evaluated (check); and the ISMS is improved based on the evaluation results (act). A graphical representation of this cycle is presented in Figure 4.3.

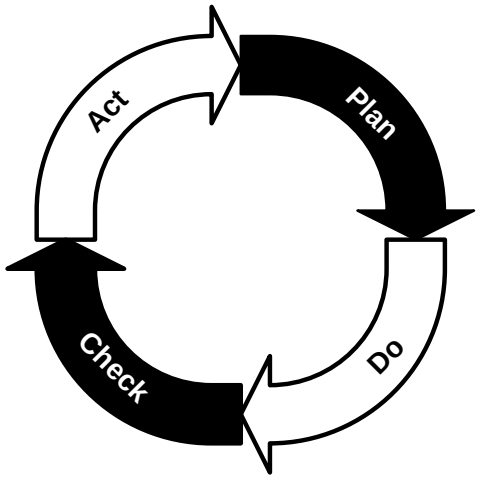


Figure 4.3: The Plan-Do-Check-Act cycle (source: ISO 27001). In this model, an organization continuously improves information security following the outlined process.

An organization which conforms to ISO 27001 has established a process where information security is continually evaluated and improved. Organizations can certify themselves for this standard: an external auditor visits an organization and verifies whether the organization complies with the requirements.

4.2.1.3 ISO 27002 – Code of practice for information security management

ISO 27002 describes a comprehensive collection of security controls. It provides organizations with security controls which are accepted and used by a large base of organizations, but it also states that organizations adopting this standard have to select controls based on a risk assessment. Nonetheless, the security controls that are described apply to most organizations and in most environments and can thus serve as a good starting point for developing organization-specific guidelines.

4.2.1.4 ISO 27799 – Information security management in health using ISO/IEC 27002

ISO 27799 is a standard for information security that is specifically aimed at healthcare organizations. It is an adapted version of ISO 27002 which addresses aspects that are unique to the healthcare sector.

4.2.2 Dutch national standards (NEN)

Besides the international information security standards, there are also national standards in the Netherlands for information security. These standards are maintained by the Dutch

Standardization Institute (NEN), the national standardization organization in the Netherlands which maintains all Dutch standards.

NEN has published four standards related to information security. Three of them are the translated versions of international standards from the ISO 27000 family. These standards are interchangeable with the international versions of them. One standard, which has been numbered as NEN 7510, is a specific Dutch standard which describes information security for healthcare organizations.

4.2.2.1 NEN 7510 – Information security in the healthcare sector

NEN 7510 is an information security standard which is specifically aimed at the healthcare sector. This standard is based on a draft of the ISO 17799:2000[4] standard. The security measures described in NEN 7510 are specifically tailored to healthcare organizations. The standard is applicable to all types of healthcare providers, including hospitals.

The standard explains which differences exist between healthcare organizations and other organizations. The standard highlights the combination of specific functional requirements with specific risks: it is for instance required that patient records are always and on every location available, but the information is highly confidential and incorrect or unavailable information is potentially life-threatening.

2004 version

The 2004 version of NEN 7510 was the first version of this standard that was published. This standard was based on the generic international information security standard ISO 27001, but it has been customized and extended so that it is applicable to the healthcare sector. The standard pays for example special attention to elements that describe how access to information is controlled and to 'healthcare-specific' elements.

2011 version

The original NEN 7510 standard was published in 2004. In November 2011, a revision of the standard was published (NEN 7510:2011). This revision is based on international standard ISO 27799, which is specifically aimed at the healthcare industry.

One of the criticisms on the old version of NEN 7510 was that it was mainly a set of required security measures which organizations have to take. Organizations implementing the standard therefore focused mainly on these requirements and some of them were experienced as infeasible or unrealistic. However, most security measures were mandatory. The new version of NEN 7510 made many of these requirements optional elements. Organizations are encouraged to implement these measures, but the obligation is dropped and security measures should now be taken based on an integral risk analysis in which the organization determines which risks exist and whether these risks are acceptable. When a certain risk is unacceptable, the organization should decide how to mitigate that risk and to what extent a risk is acceptable.

The risk analysis is a mandatory element of the new standard. Another mandatory element is the existence of an information security management system (ISMS). The general architecture of an ISMS is described in the standard. The described ISMS is similar to the ISMS described in ISO 27001.

During this research, almost every organization that was visited used the 2004 version of NEN 7510, as the revision was published in November 2011, after many organizations have

[4] ISO 17799:2000 was the predecessor of ISO 27002 (Code of Practice for information security management).

been visited already. However, the 2004 standard is withdrawn by NEN and organizations have to comply with the 2011 revision from now on.

4.2.2.2 NEN 7511 – Specification for use of NEN 7510 in complex organizations

NEN 7511 is a standard that was published in 2005 (one year after NEN 7510 was published) and it is a more detailed specification of NEN 7510. NEN 7510 is a generic standard for all types of healthcare providers, NEN 7511 provides a set of security measures for an organization: it is a reference and guidance for organizations implementing NEN 7510 compliancy.

To differentiate between large organizations and smaller organizations, three different versions of the standard have been published: a standard for complex organizations, such as hospitals (NEN 7511-1); a standard for cooperations (NEN 7511-2); and a standard for individual practitioners (NEN 7511-3). The standard for complex organizations contains the most severe security measures, whereas the standard for individual practitioners has the most relaxed set of security measures.

The NEN 7511 standard is superseded by the 2011 revision of NEN 7510: the revised NEN 7510 standard made a risk analysis mandatory, security measures should be based on that risk analysis and as such it is not needed anymore to have a specific implementation standard for specific types of organizations – based on the risk analysis, organizations should decide whether to implement a security measure or not.

4.2.2.3 NEN 7512 – Basis for trust for exchange of data

This standard, published in 2005, describes requirements for healthcare organizations which exchange information with other healthcare organizations. It describes a classification scheme, where information is classified on scale from low risk to very high risk. This classification is based on the chance of an incident and the impact of an incident. Based on the classification of exchanged information, the standard requires various security measures such as encryption, registration, and personal accountability. This standard is still effective after the 2011 revision of NEN 7510.

4.3 Description of the Dutch healthcare system

The Dutch healthcare system embodies a large group of medical professionals and medical organizations: general practitioners, medical specialists, hospitals, and others. General practitioners (GPs) deliver primary care in the Dutch healthcare system. When needed, a general practitioner refers a patient to a medical specialist. There are many general practitioners in the Netherlands; in 2009, there more than 8700 GPs. On average, one FTE general practitioner serves 2351 patients (Hingstman and Kenens, 2009). Medical specialists are usually attached to hospitals.

Hospitals are spread throughout the Netherlands. There are 148 hospitals in the Netherlands. 85 of them are general hospitals, which provide a broad spectrum of medical treatments. There are eight academic hospitals in the Netherlands. Furthermore, there are 32 categorical hospitals (such as cancer treatment centers, radiotherapy centers, etc.) and there are 23 rehabilitation centers (Dutch Hospital Data, 2009). Most cities have an own hospital or there is an hospital in a nearby city. Larger cities often have more than one hospital or they have one hospital with multiple locations.

A relatively new development is the emergence of private clinics and independent treatment centers. In 2005, there were 70 private clinics and 79 independent treatment centers, in 2009 these numbers were increased to 102 private clinics and 195 independent treatment centers.

Private clinics provide healthcare that is not covered by healthcare insurances, independent treatment centers provide insurable healthcare. Both types are usually small-sized (Dutch Hospital Data, 2009).

This study is aimed at general and academic hospitals (93 hospitals), excluding private clinics and categorical hospitals. The rationale behind this decision was that these type of hospitals are also not included in earlier research on this subject.

4.3.1 Organizational structure

This section describes typical structures found in Dutch hospitals. There is some variety among hospitals, however.

There are various organizational structures for hospitals, but a common structure is one where the medical specialists are not employed for the hospital. In this type of organization, medical specialists cooperate with other medical specialists in a cooperation (‘maatschap’). The hospitals pays the cooperation for medical treatments. Usually, there is one cooperation per medical specialism, but there are also hospitals which have a single cooperation for all medical specialists. In all these cases, other medical personnel is employed for the hospital, unlike the medical specialists. Medical specialists negotiate with the hospital management about the prices for healthcare provision (Schut & van de Ven, 2005).

Another scenario is that all medical specialists are employed for the hospital. However, this situation is rare; with the notable exception of academic hospitals where all medical specialists are employed for the hospital.

4.3.2 Health care reform of 2006: increasing market forces

Until 2006, the Netherlands had a system with private insurers and not-for-profit insurers (these were ‘sickness funds’). Depending on someone’s income, a person was either insured with a sickness fund (income below a certain threshold) or with a private insurance company. This system ensured that each Dutch citizen had access to healthcare and that basic healthcare costs were insured.

In 2006, a drastic reform of this system was introduced. The not-for-profit sickness funds were privatized or merged with private organizations and are now allowed to make profit. However, all insurers are since 2006 obliged to provide a basic healthcare package. The basic insurance package covers essential healthcare services, which are defined by law. Insurers cannot restrict enrollment for the basic insurance package and must accept all applicants for the basic insurance, regardless of age, gender, health status or other personal characteristics.

Furthermore, every citizen living in the Netherlands is required by law to have a basic healthcare insurance. The rates for the basic insurance are determined by the insurance companies which have to compete with other insurance companies. To ensure that also citizens with low incomes are insured, citizens with a low income are entitled to a monthly subsidy for healthcare insurance (‘zorgtoeslag’). Besides the basic insurance package, insurers also sell supplemental insurance, covering healthcare services not covered by the basic package.

The primary driver for the 2006 healthcare reform was to reduce healthcare costs: the incentive for insurers to reduce expenses was stimulated by price competition and freedom of choice (Boone et al., 2010).

4.3.3 Revision of the financial funding system

Besides a reform of the insurance system, the financial funding for healthcare providers has also been revised. Since 2006, healthcare providers are reimbursed for each single treatment. Medical treatments are registered using a special treatment code; the so-called DBC's (diagnosis & treatment combination). These treatment codes are used by all healthcare providers and are needed to get reimbursement from insurers.

DBC's are divided in two different categories: the 'A segment' and the 'B segment'. Prices for DBCs in the A segment are fixed by the government, tariffs for DBCs in the B segment are free: hospitals and healthcare providers have the freedom to define their own tariffs. Insurance companies can bargain with healthcare providers about these tariffs. Medical treatments in the 'B segment' only contain non-urgent, non-complex medical treatments. Urgent or complex treatments are categorized in the A-segment and are not subject to tariff negotiations (Knottnerus, 2007).

4.3.4 Impact for healthcare organizations

Healthcare providers have more freedom to define tariffs for medical treatments, but they are also subject to market forces. The introduction of standardized tariffs made it possible to compare an hospital with other hospitals. Insurance companies compare hospitals which each other. The legislations allows insurers to sign contracts with preferred providers only (selective contracting), and they can negotiate aspects likes prices, waiting times and other aspects (Maarse & Ter Meulen, 2006). Hospitals must therefore remain competitive by achieving cost reductions. It is already seen that this greater focus on expenses led to significant cost reductions (Nederlandse Zorgautoriteit, 2011).

Another way for hospitals to deal with market forces is a greater focus on their strong aspects. For instance, an hospital which is specialized in a certain medical treatment may emphasize this specialization. Other hospitals may instead emphasize their hospitality, or their regional location (nearby for patients), etc. (Knottnerus, 2007).

4.3.5 Increasing usage of information technology and exchange of medical data

There are currently different ongoing developments in the Dutch healthcare sector. As described in the previous sections, there are various developments related to the increased market forces and competition in the healthcare sector: this leads to a stronger focus on costs, specialization and profiling of hospitals.

However, there are also other developments in the healthcare sector. One of the most important developments is the introduction and increasing usage of information technology in hospitals and other healthcare providers. In the past decade, many hospitals have for example acquired an electronic patient records system (EPR). Some hospitals have effectively banned paper forms and paper records, and have switched to automated systems to record patient information.

A typical hospital employs various information systems, such as an Hospital Information System (HIS), a Radiology Information System (RIS), Laboratory Information System (LIS), a Picture Archiving and Communication System (PACS) for radiography pictures.

Sometimes, the government enforces the introduction of new information systems, such as with the electronic medication prescription. Doctors usually prescribe medicines by filling out a paper recipe. However, such paper recipes can get lost, they can be unreadable (the infamous 'doctors handwriting') and the paper recipe must be sent to the pharmacy. With

electronic medicines prescription, recipes can be sent to the pharmacy much quicker, in a format that is usually better readable. Electronic prescriptions make it also possible to verify possibly dangerous combinations of medicines automatically.

4.3.6 National patient records system (EPD)

To increase information exchange between various healthcare providers, the Dutch government has been in favor of a national system for patient records. This system is commonly referred to as 'elektronisch patiëntendossier' (EPD), which stands for *electronic patient record*.

The system is not set up like a central database like the British NPfIT system, but rather as a decentralized system: medical information is stored in the information systems of healthcare providers, and there is a central reference index which contains references to this medical information. The reference index itself does not contain medical data. When a healthcare provider looks up information about a patient, he will first search in the reference index to find references to patient records at other healthcare providers. When required, specific medical records can be retrieved electronically from the information system of the other healthcare provider (Van 't Noordende, 2010).

There has been many controversy over patient privacy in the EPD system. In 2011, the Dutch senate voted down a law which would make it mandatory for healthcare providers to connect to this system. The primary reason why the proposal was voted down was because of a lack of trust in the EPD system: senators feared that privacy of patients could not be assured and requested that exchange of medical information would be limited to a regional exchange, instead of the proposed national exchange (Eerste Kamer der Staten-Generaal, 2011; Webwereld, 2011a).

Despite the resistance in the Dutch senate, the EPD system will be continued in 2012, but in a different setting. The Dutch Federation of Patients (Nederlandse Patienten Consumenten Fedaratie, NPCF) announced in December 2011 that the EPD system will be continued by a private consortium of hospitals, general practitioners and patients. Health insurers will fund this system (Automatisering Gids, 2011). More attention will be paid to the privacy aspect. For instance, patients have to give explicit permission before medical information is exchanged and without a separate permission for national exchange, information exchange is limited to a regional basis (NRC, 2011; Webwereld, 2011b). At the moment of writing, there is a lot of uncertainty about the status of the EPD system and its future.

The Dutch Healthcare Inspectorate, meanwhile, advised in November 2011 that healthcare providers should exchange more medical information and should devote more attention to information management. The Inspectorate further emphasized that healthcare providers should develop standards for information exchange (Inspectie voor de Gezondheidszorg, 2011).

4.4 Information security in Dutch hospitals

In the past decade, information security has become an important topic for Dutch hospitals. This section describes some history about information security in Dutch hospitals and earlier research on this subject.

4.4.1 Early start of information security: increasing pressure

In 2004, the Dutch standardization institute (NEN) introduced a standard on information security in the healthcare sector, the NEN 7510 standard (see also the earlier section about information security standards).

Around the same time, the Dutch Healthcare Inspectorate (Inspectie voor de Gezondheidszorg) was researching how hospitals protect medical information. The Inspectorate visited twenty hospitals throughout the Netherlands and concluded that there were serious problems with information security: hospitals did not pay enough attention to the risks involved in employing information systems and according to the Inspectorate, patients could suffer from these risks (Inspectie voor de Gezondheidszorg, 2004). In 2004, most hospitals experimented with electronic patient record (EPR) systems, but the usage of information technology was limited. However, the Inspectorate expected that the amount and consequences of IT- related risks would increase because of the upcoming introduction of a national EPD system (see section 4.3.6, p. 25) and increasing usage of information technology within hospitals. The Inspectorate required that hospitals would comply with the recently introduced NEN 7510 standard and announced that it would perform a new investigation on this subject in the future.

In 2007, the Dutch Healthcare Inspectorate and the Dutch Data Protection Authority (College Bescherming Persoonsgegevens) performed a joint investigation on information security in hospitals. Again, twenty hospitals were randomly selected and visited by both inspectors of the Healthcare Inspectorate and the Data Protection Authority. The inspectors concluded that many things had been improved in comparison with the 2004 investigation, but many improvements were technical improvements – there were few organizational improvements. The inspectors concluded for instance that many security measures were not formalized in policies, responsibilities were unclear, access policies were not available at most hospitals, and awareness for information security risks among hospital personnel was insufficient (College Bescherming Persoonsgegevens & Inspectie voor de Gezondheidszorg, 2008). Most hospitals did not comply with the NEN 7510 standard, nor were the hospitals formally audited by external parties.

Because of the results of both the 2004 and the 2008 investigations, the Inspectorate decided that more attention should be paid to information security and it required every hospital in the Netherlands to deliver an action plan how information security would be improved and how each hospital would ensure to comply with the NEN 7510 standard. Many Dutch hospitals have started to improve information security because of the requirements of the Inspectorate.[5]

A further driver for improving information security is the introduction of the national EPD system. Hospitals would be required to connect to this system and compliance with the NEN 7510 standard is one of the requirements of a connection to the EPD system.

Due to both developments, there was increasing pressure on hospitals to improve information security and to comply with the NEN 7510 standard.

4.4.2 NVZ regulations

The Association of Dutch Hospitals (NVZ Vereniging van Ziekenhuizen or NVZ in short) deemed the NEN 7510 standard too strict and unrealistic. The NVZ therefore established its own examination regulations (which are being referred to as 'NVZ-toetsingsreglement'), which are basically a selection of elements from the NEN 7510 standard. These elements are used in a maturity model, where for each element a score from 1 to 4 can be obtained.

[5] The Dutch Healthcare Inspectorate is able to enforce such requirements because the Inspectorate has by law the possibility to impose administrative measures. The Inspectorate is for instance able to impose a fine or to serve a compliance order (which may order to discontinue healthcare activities). Furthermore, the Inspectorate may request the Minister of Health to impose further measures if an healthcare provider fails to comply with an imposed order (Inspectie voor de Gezondheidszorg, 2011a).

Elements are structured in five different clusters, and the average score of all elements within one cluster determines the maturity level for that cluster. The clusters used by the NVZ regulations are Policy and Organization, Employees, Physical space and Equipment, Continuity, and Identification/Authentication/Authorization. Besides a sufficient (mature) score, the NVZ regulations also require an integral risk analysis. The NVZ regulations are a selection of the NEN 7510 standard, and can therefore be seen as a relaxer set of rules compared to the complete set of norm elements defined in NEN 7510.

4.4.3 Analysis of action plans (2009)

Because of the disappointing results of the inquiries in 2004 and 2008, the Dutch Healthcare Inspectorate required all hospitals to send an action plan where each hospital had to explain how they would improve information security and how they would comply with the NEN 7510 standard. The Inspectorate collected all plans. M&I Partners (2009) performed a structured analysis on all plans (for 71 hospitals; not all Dutch hospitals were included in this study). All action plans were split out to 9 methodical domains and 13 practical domains, which were reviewed and benchmarked. M&I Partners concluded that most hospitals had an action plan which allowed external parties to audit the information security system, and most hospitals already started the execution phase. However, there were concerns about the feasibility of most plans, and a large amount of plans lacked a estimation of costs and resources.

M&I Partners also analyzed the practical implementations of all action plans. The authors searched for elements like an information security policy, improvements process, risk analysis, but also elements like firewalls, virus scanners and password policies. The authors concluded that most hospitals have an information security policy and that they are forming an organization around information security. However, the authors also concluded that the protection of personal data and compliance to data protection laws did not gain enough attention. Furthermore, hospitals often did not pay attention at all to on-line data in their security plans (M&I Partners, 2009).

4.4.4 External audits (2010)

After the 2009 analysis by M&I Partners, the Inspectorate decided that all hospitals had to send the results of an external audit in 2010, in order to show the Inspectorate the progress of information security improvement. The audits were performed by external organizations, such as auditing organizations or consultancy organizations. All audits were based on the NVZ regulations, using the maturity model. The baseline for the audits was a maturity score of 2 points or higher for all clusters.

The summarized results of these audits have not been published by the Dutch Healthcare Inspectorate, but were obtained via personal communication with an inspector. The results show that in 2010, only 41 of 92 hospitals (44,6%) had a mature score (2 points or higher) for all clusters. All other hospitals had a too low score for one or more clusters. Only 5 hospitals (5,4%) scored an insufficient score for all clusters. The cluster with the most insufficient scores was Continuity, followed by Policy and Organization. The cluster with the most sufficient scores was Physical space and Equipment.

The results of the analysis by the Inspectorate show that 55,4% of the hospitals in the Netherlands do not comply with the NVZ regulations, let alone the NEN 7510 standard. Furthermore, the Inspectorate evaluated the integral risk analysis that each hospital had to construct. The Inspectorate found that 8 hospitals did not send a risk analysis at all, and that for 35 hospitals the risk analysis was too limited and/or the risks were not balanced

adequately. This means that only 49 hospitals (53,3%) had a correct and balanced risk analysis (Vesseur, 2011).

All hospitals had to perform a re-audit when they scored insufficient on one or more clusters, to show that there is progress and that they would comply with the minimal requirements by the NVZ. At the time of writing, the results of these new audits were not available.

4.5 Summary

This chapter has provided various earlier research, literature and relevant standards on information security in general and information security in hospitals specifically. Based on the literature, it has become clear that information security encompasses more than restricting access to sensitive information: information security also includes that integrity of information should be warranted and that information systems are available when needed.

There are various standards on information security – some of them are generic standards that are used by various organizations, others are specific standards for healthcare organizations. The most relevant standard for this study is the NEN 7510 standard which is specifically aimed at Dutch healthcare organizations and to which compliancy is required by Dutch authorities. Various earlier researches have shown that Dutch hospitals do not comply with this standard. All hospitals have been audited by external organizations in 2010 and a majority did not score sufficiently for this audit. When looking at the triad of confidentiality, integrity and availability, it seems that many hospitals do not pay enough attention to the confidentiality aspect. The aspects integrity and availability are addressed more appropriately.

Based on the information that is presented in this chapter, it is possible to define a number of hypotheses (based on the research questions). These are defined in the next chapter, together with a description of the research approach that will be employed for this study.

5. Research approach

This section describes how the research questions will be answered. First, hypotheses are defined, after that, the general research approach for this study will be outlined.

5.1 Hypotheses

The research questions that were posed in chapter 3, and earlier research and related literature presented in the previous chapter allows to define hypotheses.

The main research question, *"How can hospitals improve information security successfully and in compliance with the standards?"*, implies that the security can be improved, and presumably also *needs* to be improved. This view is supported by earlier research on the compliancy to information security standards (Inspectie voor de Gezondheidszorg, 2004; College Bescherming Persoonsgegevens & Inspectie voor de Gezondheidszorg, 2008, M&I Partners, 2009; Vesseur, 2011). This leads to the first two hypotheses:

> **H1:** Information security within Dutch hospitals does not comply with the mandatory standards.
>
> **H2:** It is necessary to increase the level of information security.

The second research question – "*How do hospitals implement privacy and security regulations?"* – is a rather explorative research question. It is difficult to define a testable hypothesis for this research question – instead, the answer to this question will be a collection of approaches, security measures, et cetera.

The third research question implies that hospitals face problems with improving information security: *"Are there problems in implementing security measures?"* These problems can be of varying nature, but based on the rather large amount of hospitals that do not comply with the information security regulations and the amount of attention which is devoted to this subject by the Healthcare Inspectorate, it is possible that these problems are not only caused by a lack of security interest by the hospitals –these problems have probably a more fundamental cause. This is reflected in the third hypothesis:

> **H3:** There are conflicts between security requirements and common hospital practice.

This hypothesis assumes that some security measures conflict directly with common practice in hospitals, and that it is therefore difficult to comply with these security regulations.

When it is possible to find problems in improving security, it is quite possible that these problems are common for a representative group of hospitals. The organizational structure, practice and other aspects are common between hospitals, so one can assume that information security problems are also common between hospitals. This leads to the fourth hypothesis:

> **H4:** Problems with improving information security are common between Dutch hospitals.

Based on this hypothesis and on the last research question – *"What 'best practices' or patterns can be identified?"* – it is expected that best practices and patterns can be found. This is tested by the following hypothesis:

> **H5:** It is possible to distinguish best practices and implementation patterns.

This hypothesis is based on the assumption that when it is possible to identify common problems (H3), it is also possible to identify common approaches to address these problems. On the other hand, successful approaches employed in one hospital can be useful for other hospitals.

5.2 General research method

The nature of this study is exploratory and qualitative (versus quantitative). This study aims to identify the process of improving information security in Dutch hospitals, and to find problems which are faced by the hospitals.

This study will be set-up using a mixed-methods design. A combination of different research methods will be combined to ensure that to gather all data and information to answer the research questions and to accept or reject the hypotheses. By using a combination of methods, the same problem is also approached in multiple ways, which may gain more information compared to using a single method.

The process of information security improvement is a complex process, and it depends on many persons and departments within an hospital. Restricting the research to a single department, or to a single hospital, would severely limit the generalizability of the research (as well as the amount and diversity of data gathered). It is therefore important to include a variety of departments, functions and hospitals in the study.

Furthermore, it is important to realize that information about information security exists at various places. There are formal policies, where the hospital establishes a policy on information security, there are persons and roles who have certain responsibilities with respect to information security, and there is the practice – where it is possible to observe how employees comply with internal policies and what risks exist (or not). When considering this, it is clear that the study should (at least) look into documents and policies, opinions and facts from people involved with information security should be heard, and some observations should be made to see how in practice personnel complies to information security regulations and whether there are any risks.

However, it is also important that this approach is a relatively broad approach: it consumes quite some time to conduct such an extensive study at multiple hospitals. On the other hand, it is important to include more than one hospital in this study, to diminish effects of eventual outliers and to make this research valid for multiple hospitals (i.e., it is more generalized). Conducting an extensive study (including document reviews, interviews and observations) at multiple hospitals is not feasible, but it is desirable to include multiple hospitals in the study.

A two-phase approach is chosen to address both issues. In the first phase, an extensive study is performed within one hospital, which can be seen as a detailed case study. As many data as possible will be gathered at this hospital. The results of the case study will then act as input for the second phase: the experiences, insights and information that have been found during the first phase are the basis for a series of visits to other hospitals. These visits are relatively short, which makes it possible to visit many hospitals.

The first phase will be referred to as the ‘detailed case study’ and shall take in one single hospital. The second phase will be referred to as the ‘validation study’ and will be conducted within a representative of hospitals throughout the Netherlands. The research questions will be answered based on the results from both studies; the results of the first and second phase are presented separately.

The results of the detailed case study will be discussed individually before the results of the validation study are presented. There is no separate discussion of the results of the validation study, the results of both studies are discussed together. The reason why there is no separate discussion for the validation study is because the primary goal of the validation study is to validate the results found in the case study, hence a combined analysis of the results of both studies is more useful.

The next chapter presents the method and results of the detailed case study. This chapter is followed by a chapter for the validation study. Each chapter contains a more detailed description of the exact research method that has been employed.

After both studies have been presented, the combined results are analyzed and discussed, which finally leads to the conclusions.

6. Detailed case study

This chapter describes the detailed case study phase of the research. This phase of the research has been carried out in the Zuwe Hofpoort hospital in Woerden, the Netherlands.

This chapter will first provide a short introduction to the hospital where the case study took place and how representative this hospital is in comparison with other Dutch hospitals. After that, the research methods that have been used are described, followed by the results. The results are grouped by topic. These results are then discussed and summarized, as a prelude to the second phase of the research (the validation study).

6.1.1 About the Zuwe Hofpoort Hospital

The case study itself took place in the Zuwe Hofpoort hospital in the Netherlands. This hospital is an independent hospital in the town of Woerden, which is located in the centre of the Netherlands (nearby the city of Utrecht). The hospital is relatively small compared to other Dutch hospitals: the hospital houses around 260 patient beds and there are around 11.600 clinical treatments on a yearly basis (Jaarverslagen Zorg, 2011). The hospital has one main location (which houses a number of policlinics, an emergency department and operating rooms), and there are some policlinics in remote villages. The hospital employs more than 1150 employees (750 FTE) and around 100 medical specialists (79 FTE). The annual turnover in 2010 was more than € 77.000.000 (Jaarverslagen Zorg, 2011).

During the case study, the hospital was actively working to increase the information security level. In 2010, the hospital was audited by an external audit organization. This audit was based on the NVZ regulations (based on the NEN 7510 standard, structured in five clusters). The Zuwe Hofpoort hospital scored a satisfactory score for three clusters, but two clusters scored below the minimum score as required by the Dutch Healthcare Inspectorate which means that the hospital in total scored insufficiently. In November 2011, a new audit was performed (after this phase of the research was already finished) and the hospital now scored a satisfactory score for all five clusters.

6.2 Method

This phase of the research aims to gain deep insight into the process of improving information security; as such, as much information as possible needs to be gathered. As described in the general research approach, multiple methods will be used to gather information. The methods discussed were:

1. Interviews with hospital employees which are involved with information security;
2. Observations throughout the hospital to gain insight in security practice;
3. Review of hospital policies, documents and communication about information security.

The three approaches are discussed below. The results of the case study and the conclusions were verified with the security officer of the Zuwe Hofpoort hospital before these results were further processed. No results were modified or removed based on this discussion.

6.2.1 Interviews

Interviews were held with employees which either have a key function in the information security organization or with employees which have a medical function in the hospital (such as a medical specialist, a nurse, etc.). In total, interviews were held with 17 employees. These

employees were working in different departments. This includes medical personnel (nurses, for example), medical specialists, managers, employees of the IT department, staff and more.

The interviews were conducted adhering to a semi-structured format (see appendix A for the interview format). Some topics were discussed with all respondents, more topics were brought into discussion based on the job of the respondent, or based on the discussion during the interview.

Topics that were discussed with all respondents include how the respondent sees his or her own role on information security, which security measures have been taken at his or her department, and what problems the respondent experienced with respect to information security – both problems with enforcing security (e.g., unsupportive personnel) and problems that are a result of increased information security). At the end of each interview, each respondent was asked whether he had additional remarks or pointers for future research on information security.

Each interview took between 30 and 60 minutes. Some respondents also offered to show their department or working environment, to support their point-of-view in the interview and to clarify certain decisions or to outline problems. These impressions are also included in the analysis.

All interviews were transcribed afterwards. For most interviews, an audio recording was made and used to verify the transcriptions. These recordings were made with permission of the respondents.

6.2.1.1 Interview analysis

The transcripts of the interviews were summarized into short statements about information security. These statements were categorized in four different categories, which were based on the set of statements. The categories that have been used are:

1. General comments about information security
2. Problems experienced with information security
3. Security measures that were taken
4. Proposals to increase information security more efficiently

The summarized format of the statements makes it possible to distinguish similar statements and to count how often a certain statement was made. Also, it reduces the amount of data to analyze to a more comprehensible amount.

6.2.2 Observations

A number of observations were also made. These observations were performed by visiting an hospital department (e.g. radiology) and observing the behavior of employees with respect to information security, such as compliance to the hospital's policy on information security. The possibility to gather sensitive information (such as medical records) was also observed.

All hospital departments have been visited multiple times, except the operating rooms (OR): this department has been visited only once, because access to this part of the building is restricted.

The radiology department has been visited even more times: as part of a risk analysis, the processes, movements and employee behavior of the radiology department has been observed during one afternoon. Information about the radiology department is therefore more detailed and more comprehensive.

The following list shows the departments, policlinics and building parts that have been visited for one or more observations:

- Common parts of the building: the entrance, reception and restaurant;
- All policlinics: cardiology, dermatology, gynecology, internal medicine, neurology, oncology, plastic surgery, pediatrics, pulmonology, rheumatology, surgery, and urology;
- The OR complex;
- All wards (including intensive care unit and pediatric ward);
- Office departments (such as management departments);
- Radiology department;
- Emergency rooms;
- Hospital pharmacy;
- Facilities such as the hospital kitchen and technical medical services.

The observations were made between June 2011 and October 2011. In some cases, a picture was taken to be included in this report. Impressions were recorded using a notebook. In some cases, an employee of the department that was visited accompanied the author, in other cases, the visit was made without informing the department in advance (to ensure a realistic situation).

The results of the observations are described in section 6.3, combined with the results from the other two methods.

6.2.3 Review of documents and policies

Besides the interviews with employees and observations within the hospital, several documents and formal policies were reviewed as a additional method to learn more about the information security process at the hospital. Documents that were reviewed include the general information security policy, the results of an external audit on information security, and the integral risk analysis. Also some documents were reviewed that were not specifically aimed at information security, but are relevant for this study nonetheless. Examples of such documents are the annual report and the general emergency procedures of the hospital.

Besides a review of available documents, various meetings were also attended. The monthly meeting of the information security working group was attended multiple times. Decisions on the information security improvement process were made in this working group, and problems with the improvement process were also discussed.

6.3 Results

This section presents the results of the case study at the Zuwe Hofpoort hospital. First, some results from the interviews will be presented. The next section presents the results per topic: it was possible to cluster all information to certain topics, in order to clarify the results and to make them better understandable.

This chapter ends with a discussion section. In this section, the results are summarized and the implications of the results are discussed.

6.3.1 Results of the interviews

As described in the previous section, all interviews have been transcribed and were analyzed by extracting various statements from them. The respondents' views on the topics that were

discussed in the interviews are summarized through these statements, and on the other hand, it is possible to have an indication of the most important views which are shared by the respondents. Furthermore, the amount of data that needs to be analyzed is reduced to a more comprehensible amount.

In total, 338 statements were counted, resulting in a total of 148 unique statements. 16 interviews were taken with 17 respondents (one interview was taken with two respondents). On average, from each interview 9.25 summarized statements were extracted.

Most statements were made by only one person (i.e., the statement was counted only once). This was true for about half of the statements: 75 statements (50.7%). All other statements were stated by more than one person. The statement frequency table follows a exponential decay pattern (see Figure 6.1). This means that there are very few statements that have been named by most respondents and that most statements are named by only one or two persons.

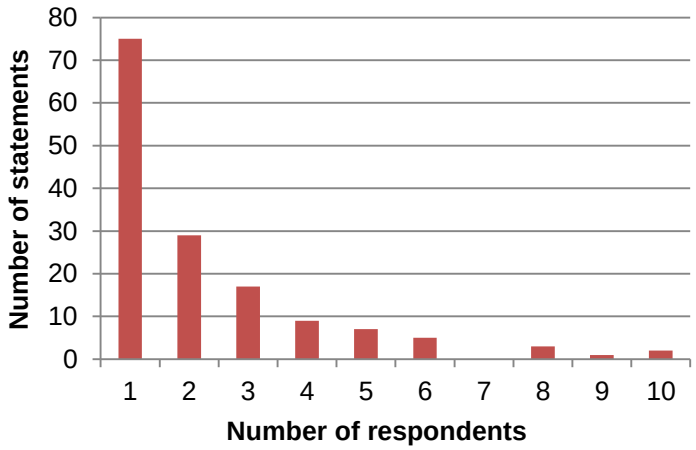


Figure 6.1: Frequencies of statements. A majority of the statements were expressed by only one respondent, few statements were made by more than three respondents.

6.3.2 Most often named statements

Table 6-1 through Table 6-4 list the statements that were named most often by all respondents, split out per category. The fact that a statement is named more often than others does not necessarily imply that these statements are more important or more correct than others, but it gives an insight in opinions that exist within the organization and may be part of the organizational culture. A full list of all statements is available in Appendix C.

Statement	Count
There is no special budget for information security	10
Progress is slowly visible	6
Each department implements the security policy in its own way	5
A change of culture is required	4

Table 6-1 General comments about information security (25 unique statements)

Statement	Count
There are no sanctions against employees breaching the IS policy	10
Employees have more care for treating patients than for information security	9

Security awareness is insufficient	8
It takes a lot of effort to comply with the information security policy	8
Behavior is the most important problem	6
Security measures are experienced as bureaucratic	6
Logging in takes too much time	6
Computers are automatically locked too quickly	5
Computer accounts are shared within a department	5
There is a tension between a safe and a workable environment	5

Table 6-2 Problems experienced with information security (66 unique statements)

Statement	Count
Technical changes (e.g., enforcing password changes)	8
Establishing a working group	6
External audit	5
Employees point out non-locked workstations to colleagues	5
Confidentiality is an aspect of the employment conditions	5
Introduction program for new employees adjusted to include a section about information security	4
There is a policy on using IT equipment	4
Internal memos have been sent on the IS and IT policy	4
An emergency plan for IT malfunction is available	4

Table 6-3 Security measures that have been taken (42 unique statements)

Statement	Count
Introduction of a sanction policy	3
Active monitoring of Chipsoft log files	2

Table 6-4 Proposed measures to increase information security (15 unique statements)

A further analysis on the interviews and the views expressed in these interviews is presented in the following section, where all data is analyzed per topic.

6.3.3 Findings per topic

The results of the interviews show how employees think about information security, which problems they mention with increasing information security or which behavior they expose which may be problematic with respect to information security.

All findings in the following section are organized around topics that can be distinguished from the results.

6.3.3.1 IT environment of the hospital

The hospital uses Microsoft Windows on all workstations. Employees have a personal account to log in to the system. This account can generally be used to access each workstation

in the hospital. Users log in by entering a username and password. A standard workstation installation gives access to e-mail and agenda (Microsoft Outlook) and standard office applications (Microsoft Office).

Patient records are stored within an electronic patient record (EPR) system. The Zuwe Hofpoort hospital uses Chipsoft. Users that need access to the EPR system have a separate account to enter Chipsoft. Furthermore, there are specific applications for each department: the radiology department employs a system to store and retrieve medical images. The pharmacy uses a special Chipsoft module for the prescription and preparation of medicines.

Most of the applications described above are available on all workstations (except when specific hardware needs to be connected to these workstations). Personal user accounts are not restricted to specific workstations or specific departments in the hospital.

6.3.3.2 General vision and vision on information technology

The Zuwe Hofpoort hospital is a relatively small hospital, which means that is has to distinguish itself from other hospitals. The hospital wants to distinguish from other hospitals by quality and costs. In order to reduce costs and improve the efficiency of the hospital, there is pressure from the board of directors to increase the production of the healthcare departments and to work more efficiently.

The Board of Directors sees IT as one of the strategic pillars to improve the quality and efficiency of the hospital. The hospital aims to work completely digital (i.e. paperless) by the end of the year 2014. This goal would be accomplished by digitizing all health processes using the electronic patient record system. Advantages of more digitization would be more efficiency, better availability of data and improved patient safety.

There are already some projects to increase the digitization of the hospital. For example, the prescription and dispersion of medicines is being transformed to a digital process. Medical specialists prescribe medicines in a computer system instead of a paper recipe and the pharmacy uses the information in the pharmacy system to prepare medicines. There are several advantages to this new approach: besides increased efficiency, patient safety is also improved. Electronic prescription systems can automatically check and warn for dangerous combinations of medicines. Unreadable recipes (the infamous doctor's handwriting) are also banned when prescriptions are digitized.

6.3.3.3 Vision on information security

The hospital has a vision on information security that is defined in the information security policy. This policy was approved by the Board of Directors in 2009 and it outlines the management system, the general policies and the principles of the information security policy. It also prescribes that the effectiveness of the information security policy should be audited internally every year. Furthermore, the policy defines that an integral risk analysis should be made and that an action plan is to be made based on the results of the risk analysis.

The goal of the information security policy is to adhere to the NEN 7511-1 regulation in 2012, and priority is given to elements that are named in the NVZ[6] testing regulations. The regulations are translated into a security plan which takes the impact of security measures on the organization into account. Risk assessments weigh security risks against limitations due to security measures.

[6] NVZ: Nederlandse Vereniging van Ziekenhuizen (Dutch Hospitals Association)

Some respondents in the interviews say that the main goal is to comply with the mandatory NEN 7510/NEN 7511-1 regulations. Some add that information security has become an issue because of the attention that is given to it by the Dutch Healthcare Inspectorate (IGZ), not because the hospitals deems it as an important topic. Very few people indicate that information security is improved to increase patient safety. The general opinion is that there are mandatory regulations from the government, enforced by the Health Inspectorate and the Data Protection Authority and that hospitals have no other choice than complying to these new regulations.

6.3.3.4 The information security management system and organization

The central part of the information security process in the Zuwe Hofpoort hospital is the management system (ISMS). The ISMS describes the goals for information security and how these goals should be reached.

The ISMS also defines that there should be a regular meeting with various stakeholders of the hospital. This meeting can be seen as a working group to improve information security within the hospital and is scheduled to take place every month. Members from various departments attend the meeting: quality assurance, human resources, IT, communication and marketing and general and technical services. There are also some managers attending, and a medical specialist to represent all medical specialists. The meeting is to discuss the implementation of security measures, but there is special authority for the working group to enforce security measures.

The ISMS prescribes an annual audit to verify the effectiveness of the information security measures that have been implemented. There have been external audits too in the past, mainly because this was required by the Dutch Healthcare Inspectorate (IGZ).

A risk analysis is required by the ISMS on a periodical basis. A risk analysis is also required when the hospital wants to deviate from the regulations; it is possible to deviate, but the risks of a deviation must be known and controllable.

The person that is the primary responsible person for information security is a staff member of the quality assurance department. This staff member advices the Board of Directors on the policy that should be adhered and watches the progress of new information security measures. The IT department was deliberately not chosen to lead this project, as the hospital feared that the approach would be too technical.

6.3.3.5 Awareness

Many respondents feel that awareness is an important issue when it comes to information security. ‘Insufficient awareness among employees’ is one of the most named problems with information security in the interviews.

The majority of the respondents indicate that employees have more interest for the patient than for information security. This is understandable, given the fact that health care workers continuously care for patients and that patient care is their core business. Health care workers are eventually assessed on their health care activities. Information security, or even information technology at all, does therefore not always gets the attention which would be desired. It does not necessarily mean that employees have no interest in information security at all or that they do not see the added value of information security, but for some employees it simply does not come to their mind that they work with sensitive information and that it is in the patient’s interest to protect this information.

Some respondents say: ‘Who would want to see this information’? This indicates that these respondents do not feel the importance of privacy when it comes to patient information.

Tension between information security and workable environment

According to various respondents, there is a tension between a secure workplace and a workable workplace. Security measures can sometimes be very strict and harm effective healthcare to patients.

An example of this observation is that employees are formally not allowed to use a computer that is logged in with the account of another employee. To use that computer, they have to log in with their personal account. However, this policy is often not followed. Employees say that they do not follow the official policy because it would take them too much time when logging out and logging in again (under another username).

Sometimes, the tension between information security and a workable environment has been mitigated by technical adjustments or by allowing exceptions to the policy. The workstations in the operating rooms, for instance, do not require users to log in with their personal account. Instead, when the computer starts, it logs in automatically with a shared account. This shared account has limited privileges and cannot be used for other workstations. This exception was chosen because physical access to the operating rooms is already restricted and because time is a critical element during medical operations; timely access to information systems prevails information security.

Healthcare departments sometimes have their own trade-offs to create a workable environment. Employees of the radiology department use a shared account to access workstations. The credentials for this account are distributed all over the department: a large notice with the login credentials was placed above almost every workstation. It even included the helpful notice that the password was changed because of the new password policy. It is clear that this approach does not follow the official hospital information security policy. Furthermore, during one observation at this department, various documents were found at easily accessible places (like unattended printers and paper recycle bins). In Appendix B, some (anonymized) examples of the documents that were found are included. The fact that it was possible to collect these documents and take them outside clearly shows that the trust in social control is misplaced.

Added value of information security not obvious

There are also respondents who say that employees do not see the added value of information security. One of them gives an example about what employees sometimes think about patient records: who would want to see that information? Another respondent mentions that employees do not see the sensitivity of the information in the patient records, because they work constantly with this information and therefore do not feel it is confident anymore. Some respondents also say that the regulations are ‘bureaucratic’ and that employees sometimes see new policies as ‘just another regulation’.

However, there are also respondents who disagree with this. Some argue they do see the importance of information security, but that they have to deal with many more regulations (imposed by the government, professional associations and insurers) and that there is pressure to work efficiently.

The earlier example that was described about employees using other’s accounts instead of logging in under their personal account is also related to this topic. Switching users takes relatively much time and for employees, the added value of switching users is not obvious.

Board of Directors’ role

Some interviewed employees say that the Board of Directors do not actively stimulate improvements in information security. The information security policy has been ratified by the board, but there is no pressure from the board towards lower management levels to

comply with information security policies. This plays a role in the awareness of information security: if the board would give some attention to this topic, lower management would also give some more attention this topic.

On the other hand, there are managers who give some attention to the subject of information security, but it varies per department. Some respondents question the actual influence of the board.

6.3.3.6 Financial budget

Most department do not have extra financial resources allocated for information security, but in most cases, this is not required either. Many improvements in information security can be achieved by adjusting processes or by extra communication and information to employees. No substantial investments are required for this. However, sometimes it would be desirable to invest in technology to increase security. Budget is required to make these adjustments.

An example where budget is lacking is in the installation of electronic locks: these locks are relatively expensive and therefore only installed on a limited amount of doors, such as the entrances to the OR complex or to the office building next to the hospital building (where patients are not allowed to come). It would be good for both physical security and efficiency to install this type of locks on more doors. These doors are now equipped with normal locks (with normal keys). Because it is time-consuming to lock and open each door throughout the day, these doors are currently left unlocked and only closed at the end of the day when everyone is going home.

There is no budget allocated to install many more electronic locks. It is therefore difficult for health care departments to increase physical security: doors which are opened often are not locked and malicious persons can easily access private areas of the hospital.

IT department

The financial situation for the IT department is somewhat different from most other departments. The IT department has to take quite fundamental technical measures to increase information security and to comply with information security regulations. There have for example investments been made into SMS authorization systems to provide secure webmail, investments in a redundant system, virus scanners, et cetera. These investments are paid from the general IT budget. The manager of the IT department says that that he formulates a budget plan for each year, and that he allocates a part of the budget for information security. The annual budget plan is submitted to the Board of Directors and usually approved.

However, the fact that there is budget allocated for information security does not imply that this budget is sufficient. Some IT employees feel that there is not enough budget available to make effective investments in information security. One persons says that for example the regulations require that every door should be secured, but it is too expensive to secure each door in the hospital with an electronic lock and that such investments cannot be made (see also the example in the previous section). One of the problems is that the Zuwe Hofpoort hospital is a relatively small hospital, which means that there are few financial resources compared to larger hospitals.

Meanwhile, the total IT budget is already one of the largest expenses on the total hospital budget, according to one of the respondents (2.4 million euro in 2010). The Board of Directors has made the strategic decision that IT is to be used to optimize healthcare processes – these investments also need to be paid from the general IT budget.

6.3.3.7 Sanctions

Almost all respondents indicate that there are no formal sanctions against employees who breach information security. At the time of interviewing, there was also no formal policy for such incidents. A generic sanction policy is being developed by the HR department.

While there is not a formal sanction policy, there have been cases where employees received a warning related to information security. One of the respondents gave an example of an employee who was working on an temporary basis and posted her opinions of patients she was treating on a social medium, visible for the entire world. The opinions could not directly be related to individual patients, but the hospital decided that this was a quite severe violation of the employment conditions and the employee was almost suspended (the employee left the organization before a sanction was taken).

Some people say that they give remarks about information security to colleagues when they see an insecure situation, for instance, an unattended workplace with a logged-in computer or medical records on the desk. This is rather in a friendly, collegial manner to encourage colleagues to work safer with information, than in a punishing way.

Respondents who are involved with internal communication with employees within the hospital also indicate this: during the course of the project, communication starts in an encouraging and collegial way. The hospital is aiming for information security to be part of the organizational culture, where employees easily inform colleagues of insecure organizations. When this is the case, it is a good time to have sanctions for insecure situations.

6.3.3.8 Behavioral problems and human factors

Employee behavior is perceived as one of the largest problems with increasing information security. Despite various technical security measures, effective information security still depends on the user's behavior. Various behavioral problems and other human factors were named by respondents and found during observations. This section describes these.

Clear screen policy

The information security policy demands a 'clear screen' and a 'clean desk' policy. This means that employees should clear their desk before leaving it (i.e., no documents or patient records lying on the desk) and that employees should lock their computer (or log out) before leaving, so that others cannot access the unattended computer.

One problem that is perceived by many respondents as a problem with information security is that employees do not lock their computer when leaving their workspace on their way to a patient or to another place in the hospital. This implies that unauthorized persons can use the computer without supplying login credentials and potentially have access to sensitive information, especially when the electronic patient record system is active on the computer.

Different observations throughout the hospital confirm this: many unattended computers are not properly locked and can be used by any person that passes by. These computers often reside in places that are accessible by patients and have no special protection to prevent unauthorized persons from entering the room.

There are various reasons why users do not lock their computer when leaving. Some deem it as 'unimportant' because they do not expect that others will access their computers (see also the next section about trust and social control). Others just forget to lock their workstation when they are paged and rushing to see a patient: all their attention is devoted to the patient. Sometimes, it is a lack of education: some users did not know that computers should be locked and how that should be done; others complete log off (which takes quite some time);

and one user locked only one software program (the EPR system) while e-mail, documents and other data were still accessible.

Trust in social control

When asked, users usually trust their working environment and they do not expect that unauthorized persons can enter their workplace or use their computer. It can be questioned whether this trust is legitimate: most working rooms in the hospital are not locked (some cannot be locked at all) and due to the public nature of an hospital building, patients and other persons can enter most areas without any problem. The most important areas that have restricted access are the OR complex (secured with badge reader), the pediatrics department (can be entered with a badge reader or by calling the reception), the pharmacy, and the office building where some administrative departments are housed. Almost every other location in the hospital can be accessed without unlocking doors.

Employees often refer to some form of social control, e.g. by saying that if some unauthorized person tries to access a workstation, he would be asked what he is doing and whether he is employed for the hospital. In practice, unfortunately, it seems that this social control system is lacking. During one observation, it was possible to work for at least twenty minutes at a computer in a work room while the observers' personnel badges were not worn visibly. Besides this observation, social control also relies on the presence of personnel in the first place and their cautiousness.

Unauthorized inspection of patient records

Another problem that is related almost entirely to human behavior is the unauthorized inspection of (electronic) patient records. Employees often inspect the patient records of family members, friends, colleagues and famous persons. This is a known problem within the hospital, and even though hospital policies do not allow employees to look into patient records if it is not necessary, it happens often and there is little enforcement of the policy. Access to patient records is being logged by the EPR system, but there is no proactive analysis of this information. Log files are only analyzed if there is a strong suspicion that there has been unauthorized access. The IT department has to gather all required information manually before an analysis can be made, and after that, the staff member responsible for privacy affairs has to find out if a person was authorized to access a certain patient record. There is no periodic audit or an automated system to detect unauthorized record access.

Proficiency with information technology

An important problem that was found during the study was that some employees have a rather limited experience with computers, according to multiple respondents and also confirmed by field observations. The amount of computer literacy varies per user, but sometimes it leads to insecure situations like not knowing about how to lock the computer (resulting in no locking at all) or locking the wrong program. Even worse, a lack of computer proficiency may also lead to dangerous situations when patient data is entered or modified incorrectly.

There is a policy to train users how to work with the EPR system (Chipsoft), but there is no structural training in place to educate employees in using the operating system, to avoid security problems (e.g. viruses or spam), etc.

Sometimes users are aware of the information security policy, but they are not aware of quick procedures which makes them adhere to this policy (e.g., they know that computers should not be left unattended, but are not aware how to lock the computer). During the observations, it turned out that these users do not give attention to information security, because their methods of ensuring information security take too much time.

6.3.3.9 Exchanging medical information with other healthcare providers

Medical information about patients is often exchanged with other hospitals, general practitioners, specialists or other healthcare organizations. It occurs often that too much information is exchanged. For instance, instead of exchanging some lab results, a complete patient record is exchanged.

There is no formal policy on exchanging medical information. The pharmacy asks patients whether they agree upon exchanging their records with other pharmacies and general practitioners, but other healthcare departments do not have such a policy and assume that patients agree implicitly on this. Medical records are not always exchanged via secure channels; e-mail, mail and fax are usual exchange mediums for patient records. Pharmacies, general practitioners increasingly use regional patient record exchange systems, but there is still much information that is exchanged via unsecure channels.

6.3.3.10 Technical security measures

The IT department has taken different technical measures to increase information security. One of the technical measures is to enforce a stricter policy on the workstations: access to unauthorized software programs, USB memory drives and local disk drives has been restricted. Another measure is the introduction of a stricter password policy; passwords must be changed and there is a minimum amount of characters. All workstations are also equipped with a virus scanner and firewall.

Measures to increase the availability and integrity of information have also been introduced. The server infrastructure is redundant. There is a main server room in the main building in Woerden; a mirror is installed in the building in Utrecht which is synchronized continuously. If the servers in one location become unavailable due to technical problems, fire, power outage or other disruptions, the servers in the other location are still available.

A backup of all systems is made every day. These backups are made on a magnetic tape; tapes are swapped each day during a week. Each week, a backup is made on tape and stored outside the building. Even if a (part of) the main building is destructed, a backup which is not older than a week is available.

Another technical measure that the IT department wants to implement is a further integration of accounts: users have had different accounts for Windows, the EPR system (Chipsoft), Outlook and PACS. The accounts for Outlook and Windows have been integrated already (so the same username and password are used for both software packages), the other systems will be integrated too in the near future. It is expected that this contributes to information security, because users do not have to remember multiple usernames and passwords and it requires less effort to log in to a system.

Some respondents indicate that there are always people who will try to work around these restrictions and that people will find other ways to use the hospital computers in ways that are not allowed or desirable. One respondent described this as a ‘cat-and-mouse game’.

6.3.3.11 Technical shortcomings

Despite the efforts in technical measures, there are some technical issues which are not mitigated yet or there are technical problems which harm information security.

Long startup and login times

One of the most important problems is that logging in to the system can take quite some time. Users complain about the time that is needed to start the computer, to log in to Windows and then to start the applications they need.

The time needed for this process was measured a few times and it seems that there is some grounding for this complaint: logging in to Microsoft Windows can take between 60 and 90 seconds; starting up and logging in into the EPR system can also take between 60 - 90 seconds. It seems that the amount of information that a user is able to see in the EPR system also influences the time required to start the system, but this is not verified.

While these startup times may (or may not) be normal for corporate Windows workstations, the process takes too long in some cases. When a user is working for a long time behind the same computer, it may not a problem that logging in and starting applications takes more than two minutes. But in the case of a specialist who is making a round trough the hospital to visit patients, waiting two minutes before a nearby workstation becomes available is too long: medical specialists have only eight minutes to visit each patient. Specialists do not want to waste this time with waiting to log in at the computer.

Long startup times are an important problem because it can make users hesitant to logging out and logging in again, for example when another user is already logged in. Using an account of another user is not allowed, but some argue that they ignore this rule and they don't want to waste too much time because of switching users.

One of the proposed solutions to avoid long login times is to use the 'switch user'-option in the EPR system. Depending on the user logging in, this can also take quite some time, up to 30 seconds (but this depends on the amount of data a user is able to see). Furthermore, it only allows logging in as another user in the EPR system, but this option does not provide access to e-mail, agenda, documents and other applications.

External e-mail is not secure

E-mail sent to recipients outside the hospital is not sent via trusted channels. There is no guarantee that e-mails are not intercepted (they are not encrypted), nor can be guaranteed that sent e-mails are delivered to the recipient and not someone else.

However, there is a need to improve the security of external e-mails. E-mail is often used to exchange information with other hospitals, with general practitioners, pharmacies and other health care organizations. It is known that specialists often exchange medical information or lab results via e-mail; all external e-mails are sent via an unencrypted channel.

There is no clear solution how to solve this problem. One of the largest issues is that all available solutions are not compatible with other solutions, so once an hospital decides to use a certain technique to encrypt or sign e-mails, all recipients have to use the same solution – otherwise signatures cannot be verified and encrypted mails could not be decrypted.

The hospital waits for the point-of-view of the association of Dutch hospitals (NVZ), so that all hospitals agree on using the same standard. Choosing a standard that is not used by most other health care organizations would not make sense, as the chosen solution would have little effect in practice.

Users trying to avoid limitations

While security policies have become stricter, there are always some users who try to circumvent these limitations. Members of the IT department however say that these workarounds are eventually found and restricted. A 'cat-and-mouse game' will probably however continue to exist.

If users have problems with the restrictions imposed and they cannot carry out their work anymore, it is possible to request an exception for their personal account. It is for example possible to request to use USB memory drives. Only after approval from the user's manager the limitations are lifted.

6.3.3.12 Organizational problems

Organizational problems also affect the effectiveness of information security within the hospital. Various respondents indicated that it is important to have commitment from the Board of Directors for taking security measures, and that it is also important that employees feel to be responsible for information security. However, sometimes, this seems to be difficult to realize and some respondents complain that responsibilities are not always clear to all functions and departments in the hospital.

One respondent says that the Board of Directors is not very proactive when it comes to information security. According to this respondent, the board should say 'comply with this regulation', but they don't do so. Also, there is not enough additional funding provided specifically for information security. This also relates to awareness among employees: the employees do not feel the pressure from the board of directors.

Medical specialists not employed for the hospital

One problem with the organizational structure of the hospital is the organization of medical specialists. Medical specialists are not employed for the Zuwe Hofpoort hospital, but they have an own cooperation. There is a separate cooperation per specialism, such as a cooperation for the cardiologists, a cooperation for the radiologists, et cetera. There are currently 23 cooperations associated with the Zuwe Hofpoort hospital. The hospital delivers patients to the cooperations, and the cooperations get paid per medical operation.

This structure is quite common for hospitals in the Netherlands. There are exceptions to this structure; there are hospitals where medical specialists are employed for the hospital instead a cooperation, but this is a minority. There is a notable exception: all academic hospitals have medical specialists employed for the hospital. Specialists working for a cooperation usually earn more wages than specialists who are employed for an hospital, and they have more freedom because they are not attached to the hospital.

The specialists cooperations cannot be held responsible for complying to all hospital policies. However, there is an admittance agreement between medical specialists and the hospital. Despite that, it is usually more difficult to involve specialists with new policies compared to other hospital employees.

Another problem that one respondent perceived as a problem is the hierarchical structure of the hospital. Feedback on changes and improvements is usually top-down instead of bottom-up.

6.3.3.13 Emergency plans

In order to continue the healthcare provision to patients, each department should have an emergency plan when critical information systems are not available. These emergency plans should contain action plans how to deal with missing information or how to record information about patients. Respondents say that there is difference between the different departments: some departments do not have an emergency plan at all, while others have a tested and effective emergency plan.

Some healthcare unit managers argue that the IT department is responsible for emergency plans, because they are also responsible for the technical functioning of these systems. The IT department, the board of directors and some staff personnel however argue that the IT department is only responsible for the technical part of emergency plans and that a healthcare unit itself is responsible for emergency processes because of malfunctioning information systems.

Some respondents say that they did not know about the existence of an emergency plan for their department, while others (from the same department) said that there is a plan available and that it is known by all employees. Others say that they have a functional emergency plan and that it has functioned correctly during interruptions in the hospital's information systems.

6.3.3.14 Communication of information security policy to employees

Different initiatives have been employed to inform employees about the existence of an information security policy, the stricter regulations on using hospital IT equipment and information systems and new procedures. One of the more formal means of communication is an internal memo to all employees that reminded them of their employment conditions and their obligations with respect to information security and confidentiality.

A more informal way of communication is via the weekly internal newsletter (distributed via the hospital's intranet and in paper), which lists short news messages about the hospital. The employee magazine (distributed monthly) provided some interviews with employees about information security. These informal ways of communication are deliberately not very stern, but rather encouraging (according to the hospital's communication manager).

A stricter way to communicate security regulations is the advertisement of IT regulations through leaflets and notices at strategic places. For example, some printers have a notice attached that reminds users of their information security obligations and not to leave their prints unattended. Security policies are also expected to be communicated by managers and team coordinators. However, in practice, this is not always the case: several employees could not remember that their manager or team coordinator paid attention to information security.

6.3.4 Structured findings

It is useful to structure the findings of the case study according to the structure of another study. It provides context to the individual findings and makes it easier to combine related findings in one category. This does not replace the findings itself: it should be seen as an additional view on the results.

To structure the results, the matrix that has been used by Krens et al. (2010) is used. Krens et al. identified seven different dimensions that are important for information security. These domains are borrowed to structure the findings of this case study. The domains are:

1. **Priority**
   How important is security (availability, integrity and confidentiality of patient information)?
2. **Incident handling**
   Is the importance of reporting incidents (system failure, confidentiality breaches, unsafe systems) recognized?
3. **Responsibility**
   Who or what is responsible for medical information security?
4. **Functionality**
   Do systems support security in daily working routines?
5. **Communication**
   How is the communication about medical information security?
6. **Supervision**
   Is the correct usage of medical systems examined?

7. **Training and education**
   Do health care professionals know how to act?

The results that have been described in the previous sections are summarized in Table 6-5. The summarized findings are the most important findings for each dimension, and for each dimension, multiple findings are shown.

The table give some structure to the findings, especially to problems that have been identified during the study. While it cannot comprise all findings and subtleties, the most important ones are included in the table.

Dimension	Findings					
Priority	Not all managers deem it important enough	Insufficient awareness among employees	Employees unaware of risks	Main goal is to comply with information security regulations	Not enough budget and resources	
Incident handling	Rather reactive than proactive	Emergencies are handled ad-hoc	There is a formal system for recording incidents	Severe incidents are reacted upon, minor incidents go unnoticed	Employees notify colleagues of insecure situations	Lessons are learned from incidents
Responsibility	Departments don't feel responsible for emergency plans	Working group is responsible, bus has little influence	Information security is sometimes seen as an IT problem	Employees rely on technical security behaviors		
Functionality	Some systems enhance patient safety	Authentication not always integrated in the existing network	Technical security measures are forced by the IT department			
Communication	Mostly one-way communi-cation	Most communi-cation tends to be quite formal	Problem is approached from the regulations, not from the patient	A working group is established to communicate new policies and procedures		
Supervision	There are no formal sanctions	Management does not reprimand employees	Supervision depends on department or individual manager			
Training and education	Lack of proficiency with computers / IT	Not enough knowledge about information risks	Training sometimes inadequate	Not everyone is educated about emergency plans		

Table 6-5: Findings structured according to the dimensions used by Krens at al. (2010).

6.3.4.1 Scores for each domain (ISEE)

Using Table 6-5 and Krens et al.'s ISEE instrument, it is also possible to determine the score of the hospital on the different dimensions. The scores in the table below are based on the findings in this field study. The possible scores are:

1. Pathologic
2. Reactive

3. Bureaucratic
4. Proactive
5. Generative

The scores listed below were assigned by the author. These scores are based on the findings and on the description of the scores by Krens et al. (2010): the best matching description of each possible score was chosen as a score for a dimension. The assigned scores for each dimension, including an average of the scores of all seven dimensions, is shown in Table 6-6.

Dimension	Score	Explanation
Priority	3 / Bureaucratic	There are plans for improvement and these plans are evaluated (which would justify a score of 4/proactive), but the priority given to the subject by the healthcare departments and the reactive response upon incidents reduces this somewhat.
Incident handling	2 / Reactive	Most incidents are handled ad-hoc: there are not always up-to-date emergency plans and if they are available, not all personnel is fully aware of them. There is no formal policy on employee sanctions for security breaches.
Responsibility	3 / Bureaucratic	Some see information security as a responsibility of the IT department, or the QA department. Some rely on technical security measures only and do not realize that they have to contribute to information security themselves too.
Functionality	4 / Proactive	Workarounds or insecure situations are being phased out and risk assessments are required (and made) for exceptions to the information security policy.
Communication	3 / Bureaucratic	Communication is for a large part in one direction and is sometimes a bit formal (referring to regulations, employment conditions, etc.). Employees are not actively involved in information security.
Supervision	2 / Reactive	There is no coherent supervision on employees: it depends on individual managers, team coordinators etc. how much attention is paid to information security and whether information security is discussed and evaluated. Sanctions are only taken by severe shortcomings.
Training and education	2 / Reactive	Some users are not proficient with computers and therefore not with information security. There are trainings for working with various systems, but basic IT knowledge is sometimes missing, leading to insecure situations.
Average score:	**2.7 / Reactive – Bureaucratic**	**There is clearly a process to improve information security and there have been many improvements already. However, the organization is not equally devoted to information security, and employees could be involved more actively in the information security process.**

Table 6-6: ISEE scores for the hospitals. Scores were assigned by the author, based on descriptions of Krens et al (2010).

6.4 Discussion

One important conclusion of the field study is that there is already much improved in the past years on information security. A variety of technical measures have been taken to ensure the integrity, confidentiality and availability of information. Organizational measures have also been taken, such as the establishment of a security policy and the foundation of an information security working group. Some processes have been improved to make them more secure. Overall, the hospital's information security is improved with obvious progress for patients and personnel.

However, there is certainly place for improvement. The case study shows that it is difficult to increase information security. This section discusses the results presented in section 6.3. At the end of this chapter, this discussion will be summarized. The following discussion serves as a basis for the next phase of the study.

6.4.1 Organization of the information security process

The hospital made a staff member of the Quality and Safety department responsible for information security. It was decided not to make the IT department responsible for information security, to prevent a too narrow focus on technical issues. Because many aspects of information security are organizational rather than technical aspects, this was a sensible decision.

A special information security working group was founded to discuss information security improvements. Despite the fact that this working group has no special authority to enforce security measures, there is a regular discussion between various stakeholders within the hospital. Risks and problems are discussed and ideally, workable security measures are the result of the meetings.

The information security policy is warranted in the information security management system, the ISMS: in a cyclic process, the policy is established, evaluated and refined. The ISMS ensures that information security is formally a part of the hospital's quality system. Practical security measures are based on the policy that originates from the ISMS, instead of ad-hoc measures. While maybe not all objectives of the security policy can be reached, it is at least possible to define priorities based on risks and costs. The most effective security measures can be taken first.

Some parts of information security are decentralized: healthcare departments should take their own security measures to ensure information security. They are, for example, responsible for changing processes or establishing an emergency plan. There are notable differences among departments: some have taken many measures to increase security, others have not. It seems – also based on findings in other areas – that it is difficult to highlight the importance of information security to various hospital departments, and as such, these departments often do not feel responsible for taking appropriate actions. The board of directors does not insist on taking effective security measures, which contributes to the lack of responsibility of these departments.

6.4.2 Awareness

One of the most important obstacles that prevents effective information security is the organizational culture and the security awareness among employees. Many employees are not aware of the risks involved with information technology in the first place, and therefore trust for example too much on the computer system, without sound preparations for IT emergencies. Some rely on the technical security measures that have been taken without any own effort for information security: they do not lock a computer when leaving because the screensaver will lock the computer automatically (which it does, but only after 40 minutes of inactivity).

The hospital aims to improve information security awareness by means of flyers, computer wallpapers with a reference to information security and other communication means, but the result tends to be temporary and not effective enough.

6.4.3 Human behavior

Sometimes hospital employees do not behave according to the hospital policies. It is relatively common for employees to look into the electronic patient records of other employees, friends and relatives, even though they are not allowed to do so. Because audition of log files is rare and a manual process, the probability that unauthorized access will be detected is quite low. Log files are only analyzed when there is a reasonable suspicion that patient records are accessed without permission.

The configuration of the hospital information system does not impose many restrictions on employees: it is possible to find information about most patients that are entered within the system. Rights are based on roles (job functions), so not everyone can see the same information. However, the system is said to be relatively 'open': availability of information is more important than the confidentiality of information. This is an understandable decision in an environment where information is critical and needs to be available, but to mitigate the confidentiality risks, abuse should be sanctioned.

6.4.4 Sharing accounts and login credentials

Accounts and login credentials are often shared among employees within a department. Usually the reason for this is that it is often faster and easier to use someone else's account (that is already logged in), than to log in with someone's own account (which takes quite some time). Employees do not always see the added value of working from their personal account and they save more time by using a computer that is already logged in, increasing their efficiency.

Some accounts are specifically meant to be shared within a group of users, the so-called group accounts. The hospital is slowly expiring these accounts, and only if there is a good reason for using a group account (supported with a risk analysis), they are left in use.

However, the problem of sharing personal accounts is not solved with deleting group accounts. Accounts are shared because the added value of a personal login are not obvious and the investment (in terms of login time) are too high. To reduce this behavior, switching users should be faster and the rationale of this requirement should be communicated.

6.4.5 Proficiency with information technology

Sometimes employees do not have much experience with using information technology and therefore do not work safely and efficiently with the hospital's information systems. This can lead to problems: these employees may avoid using the computer system (resulting in incomplete patient records or a lack of knowledge about a patient), they may spend too much time on using a computer (which is inefficient) and they can easily make mistakes without noticing them (resulting in incorrect, outdated or missing information).

It is also possible that unfamiliarity with the hospital computer systems may result in a threat to the security of the hospital information systems: an example would be opening an e-mail with a virus attached, or not knowing how to lock a computer safely, and thereby providing access to unauthorized persons.

6.4.6 Continuity

An hospital needs to provide healthcare continuously. The continuity of the information systems and the availability of patient information is therefore very important: it is difficult to treat patients effectively if their records are not available, and the risk of medical mistakes is also higher when critical information is not available or missing.

However, hospital information systems are complex systems that depend on many factors, such as energy supply and other information systems (operating system, network directory, databases and file servers). If one of these systems fails, the hospital information system (or a part of it) is unusable.

Various technical measures have been taken to ensure the availability of the hospital information systems. The server system is spread over two locations and important system components are redundant. However, despite all technical measures, the information systems

are not always available: unexpected disruptions can still occur and sometimes systems need to be shut down for planned maintenance.

6.4.7 Technical issues

While substantial technical investments have been taken to ensure the continuity of the hospital information systems, there are still some technical issues. Notably PACS, the radiology information system, was often unavailable in the past half year. Such disruptions decrease the motivation to comply with information security rules: employees are already upset that the system is not working as expected, and when it works, they do not like to be bothered with information security regulations.

The same goes for other technical annoyances. The time to log in on a workstation can be substantial and therefore it is tempting to work under the account of another user. This goes especially for employees that often have to visit patients.

6.4.8 Emergency plans and incident handling

Healthcare departments should not expect that the hospital information system is always available. The information security policy requires that each healthcare department should have an emergency plan that describes what procedures should be followed when a critical information system is not available. Healthcare departments should also take measures to minimize the impact of an unexpected system disruption: critical information should also be available via other means such as paper forms or printed documents. This would guarantee that information is also available during an IT disruption.

Emergency plans for information system disruptions are not always available and are certainly not always documented. Sometimes there is an informal, ad-hoc emergency plan, which originated from an earlier disruption, but these are not documented.

There are also healthcare departments that have no plans for IT emergencies at all: when the information system is not available for a while, healthcare processes are severely disrupted and can possibly harm patients because information is missing or not timely enough available. Most departments do not feel the responsibility to establish an IT emergency plan and argue that the IT department is responsible for mitigating problems with IT systems (see also section 6.4.1).

Incidents with information systems are registered, but this registration is primarily intended to resolve current issues and not to prevent future issues. A more thorough registration would enable the hospital to take proactive actions and to prevent disruptions of critical systems.

6.4.9 Communication

There is some communication about information security to employees, but this communication is not always effective. Some employees could not remember any communication about information security when asked. Especially communication by team coordinators or managers about information security is important, because they can adapt the abstract policy to practical security measures that are tailored to the specific department. Processes can be changed, for instance. The topic is also more vivid when it is discussed with a team rather than the one-way communication through internal memos and the hospital newsletter.

6.4.10 Organization of the hospital

The hospital has introduced a 'dual hierarchy' system: there is the hospital hierarchy, with healthcare units, staff departments and a board of directors, and there is a hierarchy of medical specialists which are organized around cooperations. Medical specialists are not employed for the hospital, but for the cooperation for which they work. This type of organization is quite common for a Dutch hospital, but it makes it sometimes difficult to introduce new policy. It is more difficult to sanction medical specialists.

Furthermore, the hospital organization is quite complex. There are many departments, divisions and specializations. Each of them has a different role towards information security and for most persons and departments, information security is only one of many other topics to which they should pay some attention – again, the hesitating role of the board of directors makes it that information security is not seen as an important topic.

6.5 Summary

This section provides a short summary of the results of the case study in the Zuwe Hofpoort hospital.

In this hospital, there has been much progress on information security in the past years. Many improvements are made; both technical and organizational security measures have been taken. However, there are still some issues with information security which the hospital needs to take care of. When considering the three aspects confidentiality, integrity, and availability (the CIA triad) which were discussed in chapter 4, some of the issues that were found can be related to these aspects (and the conflicts between them).

Information security is organized as part of the hospital's quality system. To increase information security, not only technical problems or technical measures are considered, but also more organizational issues are mitigated. While the information security working group has little authority, the discussions often result in workable solutions that are implemented. Some aspects of information security are decentralized: departments must take their own measures and there are notable differences among departments.

One important result of the case study is that many problems with improving information security have to do with the awareness of employees. Not everyone is aware of risks associated with information technology. To some extent, there is also a contradiction between information security and efficiency: some security measures harm efficiency. Employees sometimes choose for fast but insecure method to access information, rather than a more secure (but inefficient) approach. This is a clear example of the conflict between confidentiality and availability of information.

Sometimes, employees deliberately avoid the security policy, for example to inspect a patient's medical record out of curiosity and without a medical need. The approach to this problem is only reactive, not proactive: sanctions are only if taken if the offence is accidentally has brought to the attention of the management. There are few restrictions on access to patient's records (to ensure that access is available at critical moments), but there are clear signals that this open permission system is abused. Again, this is a conflict between availability and confidentiality.

Hospital employees are not always proficient with information technology. This can lead to dangerous situations when unfamiliarity with the information system leads to incomplete information or when it leads to behavior that is threatening the (technical) security of the hospital's information systems.

With respect to the availability aspect of information security, it can be said that there are few technical problems. Care has been taken to ensure the availability of computer systems and the integrity of patient data. However, there is always a possibility that information systems are not available due to an unplanned interruption or due to planned maintenance. Technical disruptions or annoyances decrease the motivation for information security.

One of the most critical problems is that emergency plans for information system disruptions are not always available and documented. The hospital's processes and the healthcare continuity can be severely disrupted in case of an IT emergency and some departments have no plan how to deal with such a disruption at all. The incident registration system is not suited (and used) to prevent future incidents, only to resolve incidents.

Communication about information security could be improved. Especially discussion between managers and employees could be stimulated, because practical implications are then discussed.

The organization of the hospital (and the complexity of it) can sometimes make it difficult to improve information security effectively. Medical specialists do not work for the hospital, making it more difficult to sanction them. Furthermore, responsibility for information security is not taken by every department or employee. A reason for this can be the hesitant role of the board of directors.

Summing up, it can be said that various security measures have been taken to ensure integrity of information. Also, various technical measures have been taken to ensure availability of information, but these measures are mostly central, technical provisions: when an information system fails despite these measures, there are few measures taken to make medical information available (and to record new information) via other means. Finally, the aspect confidentiality is the most problematic aspect of the CIA triad: abuse of information systems is often not sanctioned or found at all, and it is common for hospital personnel to use workarounds and to bypass the information security policy.

The following chapter describes the next phase of this study: the validation study, where the results of the case study are validated among a representative set of hospitals. The discussion in section 6.4 serves as input for this validation study: the problems that were found (both practical problems and higher-level problems) are validated, but also the method in which information security is organized is validated among other hospitals. Chapter 7 further elaborates on this. The results of this phase of the study return in chapter 8, where the results of the case study and the validation study are discussed in a combined analysis.

7. Validation study

This chapter describes the second phase of the study, where the results of the case study are validated by comparing the findings with information security practice in other hospitals. This chapter first describes the method that was used for this phase of the study, including a short description of the hospitals that were involved and how representative these hospitals are. After that, the results of the validation study will be presented.

7.1 Method

This phase of the research aims to validate the results that were found in the previous phase of the research (the case study at the Zuwe Hofpoort hospital). As already described in chapter 5 (Research approach), it would consume too much time to conduct multiple extensive case studies. This phase of the research therefore concentrates on validating earlier results with multiple hospitals in a less time-consuming manner: security officers (or persons with similar responsibilities) of various Dutch were approached for an interview. In this interview, the results of the Zuwe Hofpoort case study were discussed.

Hospitals that have cooperated have been contacted in various ways. Some hospitals have been contacted via personal contacts or by referral of others (e.g., a security officer who recommended contacting a security officer of another hospital). Multiple hospitals have been contacted at an information security conference at the Dutch hospitals association (Vereniging Nederlandse ziekenhuizen, NVZ). The next section will provide some insight on the exact selection of the hospitals that have cooperated and the representativeness of this group.

A semi-structured interview was conducted with all respondents. The interview format that was used is provided for reference in Appendix D. The interview mainly focused on the results of the case study: are the findings of the case study recognizable, are problems found in the case study also applicable? What measures have been taken and what are the results of the mandatory external audit?

Most interviews took between 60 and 120 minutes. There is one notable exception: two independent hospitals that actively cooperate on information security were visited for a whole day. Various employees were interviewed and multiple departments were visited. The format of the semi-structured interviews was followed, but naturally this visit resulted in richer information than most other interviews. The results of this visit are interwoven with the other results; the visit contributed many examples of practical problems and solutions to problems.

To analyze the results of the interviews, the same approach was used as in the case study: statements were extracted from all interview transcriptions. The frequencies of all statements were recorded. All statements were furthermore categorized based on the topic or on the type of statement. This summary of the interview results were used for all analysis phases. Statements were extracted for each hospital. In three cases, multiple persons were interviewed which were responsible for one hospital. In these cases, the results were merged for that hospital (there were no contradictions found between the respondents per hospital). In two cases, one person was responsible for the information security for multiple hospitals. In both cases, the respondent was able to point out the differences between both hospitals and these differences are also reflected in the set of statements that is used.

Some hospitals have opted to remain anonymous in this study, others had no problem with their results being identifiable. For the sake of consistency, all hospitals remain anonymous in the results presented here: specific findings are not linked to individual hospitals.

Most hospitals were approached with the question to conduct a survey among employees, but eventually, only one hospital actually conducted the survey and one other hospital sent the results of a survey conducted by the security officer. Because these results are not representative for the whole group of hospitals, the results of the survey were not included in this document.

7.1.1 Cooperating hospitals

16 hospitals have been included in the validation study. Hospitals of varying size have been included. For example, the smallest hospital that was visited offered 200 patient beds, the largest hospital offered more than 1300 beds. The table below lists some statistics and (public) facts about the hospitals that have participated.

Measure	Minimum	Maximum	Average	St. deviation
Amount of patient beds	200	1 320	482	298
Clinical treatments per year	7 505	44 254	21 842	11 224
Employees (FTE)	513	9 397	1 985	2 136
Medical specialists (FTE)	29	660	152	158
Annual turnover in Euros	56 094 516	1 192 608 000	228 868 256	273 753 189

Table 7-1: Annual figures of 2010 of the cooperating hospitals (Jaarverslagen Zorg, 2011).

7.1.2 Representativeness

There are 85 general hospitals and 8 academic hospitals in the Netherlands (Dutch Hospital Data, 2009), summing up to 93 general and academic hospitals in total. 15 general hospitals (17.6% of all general hospitals) and 1 academic hospital (12.5% of all academic hospitals) participated in this validation study.

Special care has been devoted to the selection of hospitals in order to have a representative group of hospitals. The hospitals that have cooperated in this part of the study are not only geographically spread over the Netherlands, but they are also a mix of small, medium-sized and large hospitals. Furthermore, about half of the hospitals (56.3%) are located in densely populated areas (such as large cities); the other hospitals are located in smaller towns in rural areas.

The participating hospitals are located in seven of the twelve provinces of the Netherlands. 9 hospitals (56.3%) are located in the provinces of North- and South-Holland and Utrecht, which together form the most densely populated area of the Netherlands (the ‘Randstad’). There are no hospitals from the eastern, the north-west and the south-east parts of the Netherlands. It should not be expected that this is problematic for the representativeness of this study. Important factors that are related to the geographical position of an hospital, such as the region (rural area or urban area) or the size of an hospital, are already accommodated.

The mix of hospitals is also reflected in the annual figures that are provided in table Table 7-1. For example, the number of patient beds ranges from 200 beds (smallest hospital in this study) to 1320 beds (largest hospital in this study). The largest Dutch hospital offers 1339 patient beds, the smallest hospital offers 138 beds (Jaarverslagen Zorg, 2011). Most hospital sizes have been covered in this research.

Another indicator to find the representativeness of the hospitals in this study is by comparing some information security metrics with the metrics that are available from other sources (which cover all hospitals). For instance, it is known that around 38% of the hospitals has an

insufficient integral risk analysis (Vesseur, 2011). Each hospital in this study was asked whether they had an sufficient risk analysis. Five of the sixteen hospitals answered that they had an insufficient risk analysis, which is 31.3% of the hospitals within the study. While the percentage is not complete equal, it indicates that the set of hospitals is representative for all Dutch hospitals (on this area).

Furthermore, three hospitals in this study were visited for the investigation by the Dutch Healthcare Inspectorate and the Data Protection Authority in 2008, which is 18.8% of the hospitals. The inspectorate visited 20 of 92[7] hospitals in the Netherlands, which is 21.7% and therefore also comparable with the percentage in this study.

One academic hospital participated in the research (6.3%). Compared to the percentage of academic hospitals in the Netherlands, this seems also a representative percentage (8.6% for the entire country).

7.2 Results

In total, security officers of 16 different hospitals were interviewed. All interviews were transcribed and statements of the transcriptions were extracted to a table, organized per topic. The full list of statements is available in Appendix E. In total, 283 unique statements were counted. These statements were made on 1248 occasions: one unique statement was named 4.4 times on average. Per hospital, on average 78 statements were made.

Various topics could be distilled from the statements. These topics were mainly related to the interview format (see Appendix D). These topics will be used in the following sections as a structure for presenting the results.

To analyze the results of the interviews, the same approach was used as in the first part of this study: statements were extracted from all interviews and these statements were collected for all hospitals. The frequencies of all statements were recorded. All statements were furthermore categorized based on the topic or on the type of statement.

The next section describes the results per topic.

7.2.1 Hospital organization

This section describes the hospitals themselves, and the differences between the hospital from the case study and the hospitals in the validation study.

A description of the geographical location, average hospital size etc. has already been described in the previous section. Some hospitals of the case study are very comparable: they have nearly the same amount of patient beds and a comparable amount of clinical treatments.

However, there are also hospitals that are considerable larger than the Zuwe Hofpoort hospital from the case study. These hospitals do not only offer more patient beds and a larger amount of clinical treatments, but the amount of employees and the size of the physical building (or buildings) also increase. The larger hospitals in this study often have a secondary location (or sometimes even more locations) where clinical treatments are offered.

Every hospital in the study used an Hospital Information System (HIS). However, the majority of hospitals indicate that many processes use paper records and paper forms (68.8%). A minority of 25.0% indicates that a part of the processes have been fully digitized (i.e. not using paper anymore), and that the other part of the processes are still based on paper records.

[7] In 2008, there were 92 general and academic hospitals in the Netherlands, which explains the difference with the number of 93 hospitals that is used in this study (Dutch Hospital Data, 2009).

Only one hospital (6.3%) indicates that they are fully automated and that almost no paper records and no paper forms are being used. Some hospitals have the ambition to work without paper forms and paper records within five years.

7.2.2 Information security organization

Each hospital in the study was asked how the information security process was organized, which persons were responsible and which department, role or persons are responsible for day-to-day security decisions. It turns out that there are various approaches by the hospitals. Some have a full-time security officer, other hospitals have a part-time security officer (who has also other responsibilities) and some hospitals do not have a security officer at all. Furthermore, the place within the organizational structure (department or staff position) varies among hospitals. In some hospitals, information security is a staff function, while other hospitals make their IT department responsible for information security, and yet other hospitals make other departments responsible.

Various respondents were concerned that they would fear a conflict of interests when the IT department in their hospital would be responsible; for instance, they feared that the focus would be too technical or that other departments would see information security as an IT topic. Most respondents indicated that a deliberate choice was made to make the IT department not responsible, to prevent an eventual conflict of interests and to have a broad focus.

However, in five out of 16 hospitals (31.3%), the IT department was responsible for information security. In most of these cases, the security officers indicated that they worked in a staff function for the IT department. The involved security officers indicated that they did not perceive a conflict of interests between the IT department and the information security goals.

The rest of the security officers were either working for the Quality Assurance department, an internal auditing department, of they were working as a separate and independent staff officer (reporting directly to a member of the board of directors).

Most hospitals work with an Information Security Management System (ISMS) as described in the NEN and ISO standards. Some security officers keep record of all security measures by storing paper documents in a record, others use digital systems to record all required information.
A minority of the hospitals does not work with an ISMS, but they rather deploy the required elements of the NEN 7510 standard like a checklist (i.e., taking all security measures described in the standard).

Some hospitals have a form Computer Emergency Response Team (CERT) to take technical security measures in cases of technical disruptions, virus outbreaks or other security threats. In other cases, respondents indicated that there is usually good cooperation between the security officer and the IT department.

7.2.3 Earlier audit scores

During the time of the validation study, many hospitals just finished a new external audit as mandated by the Healthcare Inspectorate. To have some insight in the current level of information security, each hospital was asked how they scored on their re-audit and if their score was sufficient (i.e., a score of two or higher for all five clusters of the NVZ regulations). Most hospitals scored a sufficient score: 81.3% (13 hospitals) scored sufficiently; only 3 hospitals (18.8%) did not score the baseline level of two.

Furthermore, each hospital was asked whether the integral risk analysis was assessed as correct by the Inspectorate. The risk analysis of five hospitals (31.3%) was insufficient. Most hospitals with insufficient risk analyses already started performing a new risk analysis, only one hospital did not start with a new risk analysis.

Some hospitals in this study had been visited in 2008 by the Dutch Healthcare Inspectorate and the Data Protection Authority, as part of their joint research on information security in hospitals (CBP & IGZ, 2008). In that study, 20 hospitals (21.5% of all Dutch hospitals) were visited. Three hospitals (18.8%) were also visited for this validation study.

Two hospitals indicated that they were covered in news reports on information security: a news reporter requested the medical records of some patient by pretending to be a medical specialist. The medical administration then sent the medical records without checking the identity of the reporter.

Only one hospital in this study was formally certified for information security and for the NEN 7510 standard. When an organization is certified, the working of the ISMS is validated and the security measures are audited by an external organization. At the time of writing, there were only two or three hospitals certified.

7.2.4 Communication

There is quite some variation in the different communication methods that hospital have used to make employees aware of information security risks and policies. In most hospitals (81.3%) there have been extensive communication campaigns for information security. Common methods to communicate about information security are articles in the hospital newsletter or employee magazine, persuasive posters at strategic locations (e.g. printers), and showing a video about the risks of information security. In some hospitals, security officers gave presentations to specific departments (e.g. one single ward), or in other cases, security officers gave plenary presentations. In about one third (31.3%) of hospitals, security officers gave presentations to the upper and middle management. It was then up to these managers to further impose the security policy on their departments.

One hospital indicated that that there barely has been any organization-wide communication at all. This hospital chose to impose security policies using a top-down approach via all management layers instead, but without the support of any communication materials.

Some hospitals chose a rather direct method to point out insecure situations to employees: they place small leaflets or post cards when an insecure observation is observed. An insecure situation can for example be a computer that is not locked, or paper medical records that are left unattended.

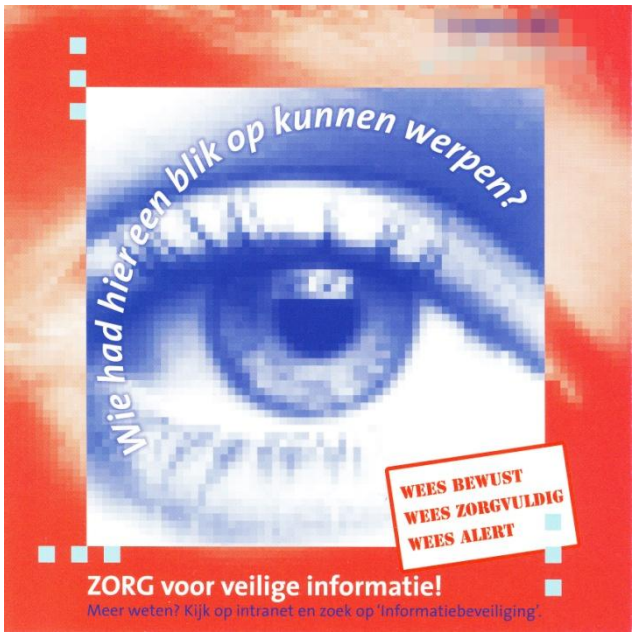


Figure 7.1: Example of a leaflet for employees, used to draw attention to sensitive information left unattended. The text around the eye says: 'Who could have seen this?' Below, the texts are: 'CARE for safe information! Want to know more? See intranet and search for 'information security'. Be conscious, be careful, be alert'.

In some hospitals, the security officer makes regular rounds through the hospital and s/he leaves leaflets and warning cards to attend employees. In other hospitals, the (physical) security department fulfills this job. One hospital even hired an employee for three months who made rounds through the building several times per week, to indicate insecure situations to employees. There are also some variations on this approach; some hospitals place a Weepul (*Wuppie*)[8] toy as a reminder for information security, and in some hospitals, positive behavior is rewarded by distributing post cards with a smiley or by some candy.

One hospital forged a phishing attack: the security officer sent an e-mail on behalf of a (non-existing) research organization, where employees were asked to enter their user name and password on an external website. About 10% of the employees responded to this e-mail and filled in their credentials. This showed that some employees were not fully aware of the risks related to phishing attacks and that they were too trustful. However, there were also some employees who reported the phishing attack to the security officer and recognized the forgery correctly. These employees were thanked by the security officer, users who filled in their authentication details received a personal e-mail which explained how dangerous it is to trust external websites and that they should not provide sensitive data to external information. The results of the phishing attack were reported to the entire organization.

25% of the hospitals indicated that there has been a communication campaign in the past, but that this campaign is now finished. 18.8% of the hospitals say that there is a continuous campaign for information security. For the other hospitals, it is not clear whether they have continuous campaigns. A pattern that is often recognized is that the amount of communication is quite high in the weeks or months before an external audit, and when the external audit is finished, the amount of communication also drops significantly.

[8] See http://en.wikipedia.org/wiki/Weepul for examples of Weepul toys.

7.2.5 Measures that have been taken

This section described the various security measures that have been taken by hospitals. Some of these measures are mandated by the NEN 7510 standard, others are to mitigate risks which became clear from the integral risk analysis.

7.2.5.1 User accounts and authentication

Most hospitals distribute personal accounts to employees. There are two hospitals in the study (12.5%) where employees do not have personal accounts, but have to work with shared (group) accounts instead. The respondents indicated that this is not a desirable situation in the light of information security, but practical and financial reasons prevent them from supplying personal accounts. For instance, hospitals would need to buy more licenses, but also constantly switching between accounts would take more and therefore more computer capacity. In one hospital, the power supply is not sufficient to cope with more computers.

In some hospitals, there is no personal Windows account, but employees work with a personal login for applications like the Hospital Information System. The permissions of shared accounts are limited: these accounts have no access to e-mail or sensitive data. Such shared Windows accounts are commonly called ‘group accounts’ and are often used when there are many employees sharing one computer. Efficient, quick access to information can be important in hospitals, for instance in operating rooms. A group account is often deployed on workstations in the operating rooms, so there is no time lost with logging in and out. The approach to group accounts is varying: 18.8% of the hospitals said they use no group accounts at all, 31.3% said that they are phasing out group accounts and 37.5% said that they will continue to use group accounts. 56.3% indicated that the continuation of group accounts is a deliberate choice.

It is possible to integrate the user accounts for hospital software with the user accounts for the operating system (directory services). Users do not have to remember different passwords and it is possible to be automatically authenticated for applications when a user is authenticated for the operating system. Furthermore, the password requirements that are enforced for the operating system are also enforced for all other applications. However, only a minority of the hospitals integrate the user accounts for hospital applications with the operating system: 1 hospital (6.3%) indicates that they do so, 10 hospitals (62.5%) indicate that they have separate user accounts for the operating system and hospital applications. For the other hospitals it was not known to the security officer whether user accounts are integrated.

Another approach to make authentication easier for user is the usage of single sign-on. Single sign-on is a technique where users log in only once and are then identified automatically for all applications they launch. 4 hospitals (25.0%) use single sign-on, 9 hospitals (56.3%) do not use single sign-on (and for the remaining hospitals it was not known to the respondent). Single sign-on makes it easier to abuse a workstation that is unattended and logged in, because all applications are automatically authenticated, but on the other hand, it relieves the burden on the user to authenticate often (which makes it more tempting to choose a rather short password, because it needs to be entered many times).

Some hospitals in the study deployed RFID or smartcard technology to secure access to workstations. Employees log in using a smartcard or contactless RFID smartcard. The smartcard eliminates the need to enter a (difficult) password; authentication is performed by inserting the smartcard or by holding a RFID card near the scanner.

Some hospitals have a terminal server set-up: employees log in onto a thin client which is connected to a central terminal server. Users log in onto one client and are able to take their logged-in session with them to another client. Sessions are switched within seconds and when

smartcard technology is used, they do not need to enter a password and can switch between workstations almost seamlessly.

However, this technology is quite expensive. Various hospitals have indicated that they would eventually like to use this technology, but they do not have enough financial resources (yet).

Most hospitals have a password policy, which requires strong passwords (as mandated by the NEN 7510 standard). Two hospitals do not technically enforce this password policy. It was not known whether employees adhere to the policy, but they are able to choose a password which does not comply with the password policy.

7.2.5.2 Permissions

During the interviews, it became clear that permissions for users are quite varying between hospitals. For 9 hospitals (56.3%), information is known about the permissions in the hospital information system (HIS).

One hospital (11.1%) indicates that employees have unrestricted access to patient records, all other hospitals (88.9%) restrict access to patient records. Employees can only access patient records when these patients are treated on the department where the employee is working for, e.g. a nurse of the oncology department can only access patient records of patients that are staying at the oncology department. Most of these hospitals (87.5% of them) also have a procedure for 'emergency access' to patient records: employees can access medical records which are normally restricted using a so-called escalation procedure. Employees have to enter to provide a reason why they are entering this record and this is logged separately. However, only two hospitals (28.6% of the hospitals with an emergency procedure) verify these logs regularly.

Two third of the hospitals (66.7%) grant medical specialists access to all patient records without further restrictions. In some cases, the respondent indicated that this is also a political discussion: who has access to which information? Sometimes, medical specialists do not want that other employees (such as nurses) can read patient records.

Group accounts usually have restricted permissions: such accounts cannot access e-mail, for example. Shared network drives are accessible however, and in some cases, group accounts also provide access to the HIS.

7.2.5.3 Employment conditions, employee behavior

Almost every hospital (87.5%) has included a confidentiality clause in their employment conditions. Furthermore, many hospitals have defined an internal policy for information security or they have integrated such policy in other policies and internal rules. Many hospitals (68.8%) inform new employees about these policies.

There are few hospitals which have a formal sanction policy for information security offences: only 18.8% of the hospitals have a formal policy for penalizing misbehavior. However, 62.5% of the hospitals respond that misbehavior is penalized – but there is no formal or standardized policy for this. The sanction depends on the manager and may vary between departments. Three hospitals (18.8%) indicate that incidents are barely sanctioned. They blame the soft organizational culture in their hospital for this.

Some hospitals have streamlined the process for hiring new employees: when the HR department registers a new employee, the IT department is automatically notified and creates a new user account very quickly. This reduces the chance that a new employee has to temporarily borrow an account from a colleague until s/he has an own account. Furthermore, half of the hospitals have improved the procedure for employees that leave the organization:

one hospital automatically disables the employee's user account when the discharge of an employee is registered, in the other hospitals; the HR department periodically sends a list of discharged employees to the IT department. Usually, this periodic list is used as a last resort and a deactivation of the account should already be requested by the manager.

Some respondents say that they have many problems with user accounts that belong to persons that no longer work for the organization, or for which it is unclear whether they still have a relationship between hospital – especially for external medical specialists who sometimes substitute internal medical specialists often do not show up for months, but they still need an active user account. It is difficult for the IT department to distinguish between users that need to have an account, but who are rarely present, and users that are no longer working for the organization. While it is usually clear for employees who are actually employed for the hospital and receive salary, this problem mainly manifests itself for persons who are not directly employed for the hospital: contractors, external medical specialists, volunteers, interns, etc. One respondent opted to link each user to a department and to verify the users of each department periodically with the responsible manager, but he has not introduced such a system yet.

In some hospitals, volunteers have no access to information systems at all (18.8%), or they see non-sensitive information (6.3%). However, only two hospitals responded that they have signed a confidentiality agreement with volunteers.

7.2.5.4 Technical security measures

Some security measures are taken by almost every hospital. It is possible to distinguish a certain baseline from these security measures. However, there is quite some variety between the other security measures: different approaches are applied and some hospitals impose a stricter security level than others.

Measures to ensure the reliability and availability of central network servers are for a large part identical. Every hospital in the study has a backup power supply and a redundant server room: if one part of the network falls out, its operations are replaced by another segment. Almost every hospital has split the main equipment rooms (MERs) over multiple locations. 50.0% of the hospitals has multiple MERs within on one location (building), 43.8% of the hospitals has MERs spread over various locations (for example an external data center or a MER in another hospital of the same organization). Almost every hospital makes a periodical backup (for the other hospitals, it was unknown to the respondent). However, some hospitals indicate that the backup restore procedure was never tested and others say that it may take a long time before a full backup is restored.

43.8% of the hospitals say that local permissions on the workstations are severely restricted: users cannot install applications or change the computer settings. 37.5% has prohibited access to removable memory drives (USB drives), which may bring in viruses. These memory drives are also harmful because users may copy sensitive information to them and then lose the drive. When a user wants to copy certain information to an USB drive, they either have to request specific permissions to do so, or they have to go to a service desk which copies the data to a secured memory drive. By doing so, these hospitals hope to minimize the risk of exposing sensitive information via memory drives.

A majority of the respondents (62.5%) configured the workstations to be automatically locked after a certain amount of time. One hospital offered users the possibility to change this locking time, all other hospitals enforced the lock time.

7.2.5.5 Emergency procedures

50% of the hospitals have a generic, organization-wide emergency procedure for disruptions in the information systems. Such a procedure describes for example how critical information can be registered and retrieved. At least 4 hospitals (25%) do not have an organization-wide emergency procedure; it is left to the various departments how to mitigate IT disruptions. 8 hospitals (50%) also indicate that various departments have no specific emergency procedure: the radiology department for instance has no predefined process for recording radiographic pictures without using IT equipment, or an intensive care unit does not know how to record critical parameters. Only 5 hospitals (31.3%) are certain that (critical) departments have defined their own emergency procedure, or they are included in the generic emergency procedure.

However, disruptions in information systems are not critical to every department. 68.8% of the hospitals say that many medical records still consist of paper records; so an outage of the hospital information system has relatively little impact for most departments.

Hospitals have taken various measures to increase the availability of electronic patient records. Not only technical measures to ensure the availability of the normal production systems are being taken (see the previous section), but hospitals also take measures to have information available in case of disruption of the (normal) production systems.

Some hospitals have a read-only version of the hospital information system available. If the normal production system needs to be shut down for maintenance, the read-only version can be made available to users. This system can also be provided in case of disruptions in the production system, like database failures.

Another approach to ensure high availability of medical records is the usage of emergency computers. These computers are local workstations which have an own power supply or are connected to the emergency power supply, and they are supplied with a local copy of the patient records database for the department where these computers are provided. Departments still have access to critical information in the event of a disruption or power outages (when network availability is not always guaranteed).

Furthermore, various hospitals have paper forms available to record critical information when the normal systems are not functioning. Some information is printed out regularly, as a backup for the information stored electronically. One hospital gives an example where the pharmacy prints out all orders for the following workday: if the pharmacy systems are not functioning correctly the next day, they can still process many orders. When the disruption takes longer than a day, there is time enough to prepare additional measures to maintain services.

Various hospitals have either critical workstations or network components not connected to emergency power supply, or there is no such information available. It is therefore possible that access to information is severely restricted in case of power outage.

7.2.6 Proficiency with information technology

A large majority of the respondents (81.3%) recognized the finding of the case study that employees have severe difficulty with information technology and a lack of proficiency with it. Nonetheless, only one hospital (6.3%) said it offers training for generic software (i.e., Microsoft Windows or office suites). If any training is provided, it is usually for specific hospital software, but employees are not trained for working with basic software and basic components.

7.2.7 Experienced problems

While hospitals have taken many security measures to improve information security, they experience also a variety of problems that prevent effective improvements. These problems are of varying nature: it can be physical problems, technical problems or organizational problems. The most important problems are discussed here.

The most important problem (which is experienced by at least 62.5% of the hospitals) is that logging in onto Microsoft Windows consumes much time. In some cases, it may take a user up to five minutes to log in onto Windows. Many respondents experience this as a serious problem for improving information security: it discourages users from switching accounts when working on a shared computer and there is a risk that the computer is being left unattended for a while during the login procedure.

Some hospitals face physical problems: they are housed in a building that is some decades old and that does not always meet up to modern requirements. There is sometimes no space to provide extra computers, or the building makes it difficult to close certain departments for visitors (because patients and their visitors also need access to many parts of the building).

Sometimes there are organizational problems that prevent effective information security. Some hospital indicate that there are financial problems and that they have too little funding for security measures. In one case, the board of directors decided that there will be no budget for information security, which effectively blocks certain new security measures to be taken.

Many hospitals (50.0%) indicate that they have problems with external suppliers: some IT suppliers are not cooperating with the security officer and are unwilling to adhere to an hospital's security policies. An example is that the hospital needs to wait a long time before important security patches are distributed, or that suppliers have a maintenance environment which is not safe enough (and does not comply with the hospital's policies). Only two hospitals (12.5%) indicated not to have any problems with their suppliers. Improving this situation is problematic for some hospitals; existing contracts sometimes prevent requiring additional security measures (because these are not specified in the existing contract) and some hospitals – especially smaller ones – indicate that their negotiation position is weak.

7.2.8 Incident registration

A majority of the hospitals record incidents: 9 hospitals (56.3%) record incidents in a registration system. However, 4 hospitals (25.0%) do not record incidents, although this is required by the NEN 7510 standard. When incidents are registered, the security officer usually starts an investigation to analyze the incident and eventually take (new) security measures.

There is some variety in the way incidents are recorded: some hospitals link the registration of incidents to the support system used by the IT department (where also incidents involving malfunctioning printers, software problems, etc. are reported). Others use a separate system

7.2.9 Information exchange

Only 6 hospitals (37.5%) have a formal policy for exchange of medical information with other healthcare providers (such as other hospitals). 31.3% of the hospitals have security requirements for the external party. However, many respondents indicated that medical specialists also often exchange medical information by other means, such as e-mail or fax.

7.2.10 Decentralized applications

Many hospitals (81.3% of them) have 'decentralized applications' – that is, software applications of which the administration is delegated to a business department instead of the central IT department. For instance, the radiology department maintains the configuration of a radiology software package (PACS). Only 30.8% of these hospitals also have a special security policy for decentralized applications. The rest of the hospitals have no special policy for these applications. However, 69.2% (9 of 13 hospitals) have security requirements for decentralized application maintainers.

7.2.11 Other impressions

At the end of each interview, all respondents were asked whether they had additional comments or remarks in the light of information security.

One remark that was made by many respondents (43.8%) is that the new NEN 7510:2011 standard is an improvement compared to the older NEN 7510:2004 standard. Multiple security officers recommended that a security officer should be pragmatic: it is not possible to mitigate every risk at once, and on the other hand, not every risk has an equal impact. A security officer should therefore mitigate the risks with the highest impacts first, or risks which are relatively easy to deal with.

What is also expressed by some security officers (and implicitly meant by some others) is that the integrity and availability of information is more important that the confidentiality of it. Of course, it is important to protect information, but ensuring that critical information is reliable and always available is more important in the hospital domain, is the consensus.

7.2.11.1 Examples of security incidents

Various hospitals have provided examples of information security incidents. Some of these also had serious consequences for either the operations of the hospital, or for patients whose privacy was compromised.

Multiple examples were provided of disruptions in the hospital's information systems. The nature of these disruptions was varying (e.g. power outage, fire, unsuccessful software upgrades, etc.) but in some cases, these disruptions had a severe impact on the hospital's operations. One security officer provided an example where information systems were not accessible for a few days due to another incident. The hospital used paper medical records, so access to these records was still possible. However, the hospital did not realize that the schedules of employees are quite critical for the hospital's operations. The hospital faced various difficulties with scheduling employees for the next days. Another problem was that all backups were almost a day old (backups were made each 24 hours): this proved to be too old. As a consequence of the incident, the hospital increased the amount of backups and the importance of the employee scheduling system has been increased.

Two security officers shared (independently) an identical example which: a nurse contacted the security officer to notify that the mobile telephone number of a well-known Dutch artist was stored in his patient record. The nurse reporting this was given a warning because s/he was obviously accessing the patient record of the artist without a medical need and without permission.

Another security officer told about a case where a patient's privacy was seriously compromised. The patient – a woman – had visited the oncology department of the hospital and heard that a malignant tumor was found on her breast. An employee of the hospital saw the woman at the oncology department and knew her indirectly. The employee wondered why the woman was leaving the oncology department and looked up her medical records, where

she found out about the tumor. The employee felt sorry for the woman and decided to send her a bucket of flowers.

The woman in question went home and decided not to tell her husband and daughter about the tumor that was discovered, as she did not decide on a treatment yet and her daughter had to pass an important exam the following day. Instead, she would inform their family a few days later, when she had decided which treatment to follow and when her daughter had made the exam. However, later that evening, the bucket of flowers was delivered to her home. The woman's husband accepted the flowers and read a card inside that was aimed at his woman. Of course, the woman now had to explain the situation to her husband and daughter, who were upset by both the bad news itself and the fact that they were not informed while a distant acquaintance was already aware of the news. The daughter failed her exam the following morning.

The woman filed a complaint against the hospital. The employee who sent the flowers was reprimanded. Of course, she had the best intentions with this action, but she did not realize the consequences of it. The hospital now uses this example to explain to new employees how careful one should be when processing sensitive medical information.

7.3 Summary

This chapter presented the research method and results of the validation study. A series of interviews with security officers of 16 hospitals was performed to find out whether the results found in the case study were representative. Most of the hospitals that were visited have scored sufficiently for a mandatory external audit.

There was some variety found in the way hospitals organize information security, especially in the hospital department that has been appointed responsibility for information security. Cooperation with other departments is usually not a problem.

In many cases, extensive communication took place to inform employees about security measures. Many hospitals have used communication material like posters and leaflets. About one third of the hospitals informed management via presentations; another minority of the hospitals informed all employees via presentations. Also other methods to communicate the information security policy and security measures were used.

All hospitals had taken provisions to ensure that information is backed up regularly and each hospital had installed an emergency power supply. However, it was found that many hospitals do not have specific emergency plans to accommodate unexpected disruptions in an information system (as was the case in the case study). Often, the status of these plans is also unsure; in various hospitals, the security officer does not know for sure whether healthcare departments have an up-to-date emergency plan that is known by the responsible employees.

Insufficient proficiency with information technology is a widely recognized issue. Surprisingly, only few hospitals offer general training on IT systems. Most hospitals only offer training for specific medical software (such as an HIS), but there is little to no attention for basic computer proficiency.

Another issue that is widely recognized is a lack of cooperation from external suppliers. While this is not an issue for all hospitals, half of the hospitals say that their suppliers are often unwilling to improve information security.

Exchange of medical information with external healthcare providers is often not formalized through a policy and only one third of the hospitals have security requirements for exchange

systems. Medical information is often exchanged via (unsecured) generic-purpose communication systems like e-mail, fax or postal mail.

This summary concludes the presentation of the validation study. The following chapter, chapter 8, analyzes the results of the case study and the validation study. Common patterns are identified, and the results of both studies are analyzed from a higher-level perspective.

Chapter 9 presents the conclusions of this study and answers the research questions. Also some recommendations for future work are provided.

8. Analysis

This chapter discusses the results that are found in both the case study and the validation study. For both phases of the research, the results have already been presented and discussed shortly. This chapter mainly focuses on the results that are similar between the case study and the validation study – i.e., the results that are applicable to multiple Dutch hospitals.

The analysis that is presented here will be a bit more structured than the results sections of both the case study and the validation study: the results are structured according to the domains described in international information security ISO standards (see further). Using this methodology makes it possible to see whether the results are covered by these domains (e.g., how complete are the results presented here?). After the structured analysis, a higher-level analysis is performed.

Before the results of the analysis are presented, it is important to know that it is very difficult to compare the effectiveness of the security policies and security measures that have been introduced by the various hospitals. The methodology of the study did not allow for comparison of the *effectiveness* of the individual policies – that was not the goal for this study. Each hospital was asked whether they scored sufficiently in the latest external audit. This provides some insight, but there are some points which should be taken in mind. First, a majority of the hospitals had a sufficient score (76.5% of the hospitals), with little difference between the individual scores. Besides that, the document which describes how these audit scores should be calculated (the NVZ regulations) explicitly warns that these audit scores should not be used to compare hospitals with each other. A further argument why comparison based on the individual audit scores is problematic is the fact that these audits have been performed by different external organizations. A standard, formal methodology to perform such audits does not exist, which implies that the score depends for a large part on the interpretation of the external auditor.

8.1 Structured analysis

As already described in the literature and theory chapter, there are various standards on information security. An example is the NEN 7510 standard, which has been referred extensively. This standard is based on the international ISO 27999 standard, which is in turn based on the ISO 27001 standard: a generic standard describing information security, being used by various organizations all over the world. ISO 27001 defines eleven categories for information security, which are also used in all other ISO standards for information security (including ISO 27799) and – in a translated form – in the Dutch NEN 7510:2011 standard.

The reason why the structure of ISO 27001 is used is that the categories used in this standard are more extensive than the CIA model (which only covers three aspects, or five aspects when using an extended version of it). The aspects covered by the CIA triad are also reflected in the categories used by ISO 27001, but ISO 27001 provides additional categories which makes that it covers a larger part of information security. In the analysis of the case study, the model of Krens et al. (2010 was used. This model is not used here because the model of Krens et al. omits some important aspects (such as the organization for information security). Finally, by structuring the analysis according to categories defined in the ISO standards, it is better possible to compare the results of the analysis with requirements of standards.

ISO 27001 defines the following categories:

- Security Policy
- Organizing Information Security

- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information Systems Acquisition, Development and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

It would be interesting to see if the results that are found fit in these categories. If there are none or only few results for a certain category, could it be that not enough attention was paid to this category in this research. On the other hand, if there are many results that do not fit in one of the eleven categories, could it be that the categories in ISO 27001 are too limited, or that there are at least aspects that are not covered in this international standard. Furthermore, using the ISO categories makes it easier to compare the results of this research with mandatory elements of the regulations: it makes it easier to find which requirements are difficult to fulfill.

The following sections discuss the results; each section is an ISO 27001 category. Each section starts with the objective that is stated in ISO 270001. Note that ISO 27799 (which is specifically aimed at the healthcare sector) contains the same objectives; the Dutch NEN 7510:2011 standard also includes these objectives (translated to Dutch).

8.1.1 Security policy

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

This category mainly includes the organizational goals and vision on information security – what goals does an organization try to achieve, which level of security is pursued, and by which means does the organization achieve this level? And how does the organization ensure that the security level is maintained in the future?

A majority of the hospitals do have a policy on information security which outlines the goals, a global planning and a schedule for periodic review. Most organizations do not distribute the complete security policy to employees, but rather a summary of it in the form of leaflets, posters and other communication material. This ensures that the most relevant elements of the security policy are communicated to employees.

Some hospitals do not have a clearly defined security policy or the goals for information security are unclear. In multiple hospitals, compliance to NEN 7510 was being referred to as the main goal for information security. This goal is somewhat vague: it is possible to comply with the minimum set of required elements defined in NEN 7510, but to fully comply with the NEN 7510 standard it is also required to maintain and improve the level of information security continuously. Various hospitals have indicated that efforts for information security will be minimized after the hospital has scored sufficiently on the required audit, which means that there is no continuous improvement of information security in those hospitals.

Both the literature and some security officers recommend that information security must be seen as a continuous process: security measures and risks need to be evaluated constantly, because both the risks and the effectiveness of the security measures are constantly subject to

changes. It is not sufficient to take a certain set of measures now without evaluating them on a regular basis.

8.1.2 Organization of information security

Objective: To manage information security within the organization.

This objective describes the organization of information security within the organization. Which departments, roles or job functions are responsible for information security? How is the management committed? In what way is the established security policy executed?

8.1.2.1 Information Security Management System

This objective is clearly linked to the concept of an information security management system (ISMS). The ISMS described in ISO 27001, ISO 27799 and NEN 7510:2011 provides a framework to analyze risks, define security measures and to evaluate these measures. The management system is centered around the Plan-Do-Check-Act cycle (PDCA cycle), which is the central process to improve information security (see also section 4.2).

While this system is not described in the 2004 version of the NEN 7510 standard that has been required until now, it is an element of international ISO security standards (ISO 27001, ISO 27799) and it has also been included in the 2011 revision of the NEN 7510 standard. This element is becoming mandatory for hospitals (assuming that they would have to comply with the 2011 revision of the NEN 7510 standard).

As seen in the results from the validation study, most hospitals already work with a system comparable to the ISMS described in the standards. However, some hospitals do not work with an ISMS. In these hospitals, security measures are usually not evaluated periodically and security measures are often being taken without a thorough base for them, such as a risk analysis. The security elements described in the NEN 7510 standard used as a checklist. While the security measures taken are maybe effective, there is the risk that the effectiveness decreases in time due to changing treats and new risks – there is no periodical evaluation and adjustment of the security policy. Furthermore, it is difficult to know whether all risks are covered by security measures and what risks are accepted. There is also the risk that an organization takes too many security measures compared to the amount of risks, or that an organization focuses on taking certain (costly) security measures which are barely effective.

8.1.2.2 Responsibilities

Another aspect of this category is the assignment of responsibilities to persons and departments within an organization. This is an interesting aspect, because there is many variation among the hospitals: especially the position of the security officer within the organization is quite different between hospitals. It is possible to distinguish rather technical positions (when security officers are working for the IT department), strategic positions (when positioned directly under the Board of Directors) or positions which have experience with organizational change and monitoring quality (such as internal auditing department, quality and safety department or an innovation department). The following list gives an overview of the positions of the interviewed security officers (including the security officer of the hospital in the case study).

- **Strategic position (38.8%)**
    - Independent staff function (22.2%)
    - Advisory function (16.6%)
- **Non-technical position (33.4%)**
    - Quality and safety department (16.6%)

    - Environment and working conditions (5.6%)
    - Innovation and organization (5.6%)
    - Internal auditing and control (5.6%)
- **Technical position (22.2%)**
    - IT department, strategic level (16.6%)
    - IT department, operational level (5.6%)

It could be expected that in hospitals where a member of the IT department is responsible for information security, there would be a strong focus on technical security measures and other organizational measures would be neglected. However, this does not seem to be the case: there are some hospitals where there is indeed a focus which is strongly oriented on technical measures, but this also occurs with hospitals where the information security officer has an independent position. Many hospitals fear that when the IT department is responsible for information security, the focus would be too technical, but this fear is not completely justified with the results.

What does seem to be important is how the responsibilities are imposed. In some hospitals, information security is an unpopular topic: sometimes even the responsible person dislikes the subject. It is not surprising that this seems to influence the effectiveness of the security policy. Related to this is the role of the upper management and the Board of Directors. There seems be a relation between the support given by the Board of Directors to information security, and the effectiveness of the organization's policy. There are clear examples of these in the study, both of organizations with a supportive Board of Directors and a relatively painless process, and organizations with an unsupportive Board of Directors and many problems related to information security.

This finding may also be unsurprising, but it stresses the importance of support from upper management.

8.1.2.3 Involvement of other departments

Not only support from the upper management is important. Other persons and departments within the organization are also important to reach information security goals: processes need to be changed, employees need to become aware of risks, etc. There are various approaches to involve other departments with information security, but there are two main approaches:

- Involving others when needed, without the establishment of a special working group or project group;
- Establishing a working group which represents some or most departments within the hospital.

There does not seem to be a method which works better over the other method, the best approach presumably also depends on (the size of) the organization. Especially small hospitals seem to favor working groups, the results for the larger hospitals are varying. The advantage of a working group is that it is possible to discuss the approach on information security within a representative group, but the disadvantage is that this approach can be time-consuming and it is not always necessary to discuss certain security measures with a large group of representatives.

8.1.3 Asset management

Objective: To achieve and maintain appropriate protection of organizational assets.

This aspect of ISO 27000 describes that all 'assets' (defined in ISO 27001 as 'anything that has value to an organization') should be clearly identified and maintained. Each asset should have an owner: an entity within the organization that is responsible for the production, maintenance and security of the asset. For instance, an information system for the radiology department is an asset, and the owner could be the manager of the radiology department.

For information systems and other assets which are centrally maintained, it is usually clear who is the owner (and who is responsible for the asset's information security). However, the study indicates that many hospitals have problems with identifying applications that are not centrally maintained (the 'decentralized applications'). Because hospitals have difficulties with identifying these applications, they are sometimes unknown to the security officer and their security risks are not known. Often, measures to secure these applications are also unknown or missing.

8.1.4 Human resources security

Objective: To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.

The human resources aspect is an important aspect: one of the primary results of the case study was that security awareness among employees is an important problem and this result was also seen in the validation study. The formal part of this category (i.e., employment contracts) is usually not problematic for the researched hospitals; most of them had adjusted the contracts and existing employees were informed about their responsibilities with respect to confidentiality. However, as said, making employees fully aware of information security risks is more problematic. Various approaches are named by respondents.

Based on the interviews with the security officers, a method where information security risks and measures are explained to a small group of employees does seem to work well. This provides the possibility to transform the generic policy to specific situations for a department or location. This method has been used by various respondents and they are enthusiast about it.

General hospital-wide presentations can take place fast and are cost-effective (a large part of the organization is informed in a short time), but the results are most of the time less satisfying. Employees may find it difficult to transform a generic policy to the specific situations which they encounter in their work, which might explain this.

8.1.5 Physical and environmental security

Objective: To prevent unauthorized physical access, damage and interference to the organization's premises and information.

This aspect is clear: it focuses on the physical security in hospitals. Hospitals are public buildings and most parts of the hospital buildings can be accessed without effort. This makes it difficult to implement a high grade of physical access security. Most hospitals in this study have already secured various parts of the building: the operating rooms are usually not accessible for visitors, and also office buildings or office departments have restricted access. However, most parts of the building are not locked and it is difficult to lock these. Multiple respondents indicated that they rely on social security: hospital employees are expected to approach unauthorized persons or visitors that they do not know. This is a risky approach in terms of information security; when the employees are busy in another room they are unaware of visitors and a typical hospital receives many visitors per day, which makes it difficult to

recognize each visitor. It is important that the hospital does not rely only on social security, other security measures are necessary for effective information security.

8.1.6 Communications and Operations Management

Objective: To ensure the correct and secure operation of information processing facilities.

This section describes many controls on the operational procedures, documentation, planning, agreements with third parties, but also various requirements on backup procedures, network security, et cetera.

What can be extracted from the results is that many hospitals have taken technical security measures to comply with the regulations. There is a certain base level which is applicable to every hospital that has been researched: each hospital has a backup power supply, a backup procedure, and a redundant network. Most of the hospitals have restricted local permissions on workstations severely and have installed firewalls, virus scanners and spam filters to protect the network and computer systems attached to it.

These are mostly measures on a operational level. When looking at a more operational level, it seems that there is a difference between hospitals when it comes to documentation, procedures, separating test and production environments and formalizing agreements with external suppliers. For instance, there are hospitals in this study which have introduced change management and have separate testing, acceptance and production environments. Furthermore, changes in the applications or hardware environment are documented and tested first. Implementing changes is a formal process and approval is required from other users before a change is implemented.

The method described above is rather formal way to maintain information systems. There are also hospitals which employ a more informal way to maintain the systems. Changes are not always documented or it may be difficult to revert to earlier system states in case of technical problems. Agreements with external suppliers are not always clear, nor are the supplier's responsibilities on information security.

The findings above mainly have to do with the maturity of the IT department within an organization. Various respondents indicated during the interviews that many hospitals have an immature IT department or that only since a few years the IT department has professionalized. These respondents see maturity of the IT department as a critical factor for effective information security, especially for maintaining integrity and availability of the information systems.

8.1.6.1 Exchange of information

When it comes to exchange of medical information, there is variety between the researched hospitals. Some have no policy on information exchange at all, others have a general policy and some have a rather detailed policy. In the latter case, medical information is only exchanged with other organizations when these organizations comply with certain requirements which are set by the hospital (both technical and organizational requirements). Only after approval by the Board of Directors information is exchanged.

A rather informal and personal way to exchange medical information with other organizations is via e-mail. Almost every hospital agreed that they are aware that employees exchange medical information via e-mail. However, only few hospitals have implemented a system for secure e-mail. There is a clear problem in this area: there are some solutions for sending and receiving e-mail in a secure manner, but these solutions are not compatible with each other and most hospitals do not use any solution at all. Only if both parties use a compatible system, information can be exchanged securely. Hospitals are investigating the possibilities and

limitations of secure e-mail and are trying to find a common system via the Dutch Association of Hospitals, but this is not realized at the time of writing.

8.1.6.2 Monitoring

Most hospitals do not employ thorough logging and auditing systems. When log files are kept, it occurs often that these log files are not analyzed afterwards: for instance, most hospitals have an emergency procedure to allow employees to access patient records for which they are not authorized normally. However, the usage of this procedure is often not verified. There are positive exceptions to this finding, but there are many cases where the security officer indicated that log files are often not checked for malicious usage.

8.1.7 Access control

Objective: To control access to information.

Some hospitals face difficulties with employees that are leaving the organization. Sometimes the IT department is unaware that these persons have left the organization and the user accounts belonging to these persons are left intact, which is not desirable.

Various hospitals have introduced a system where the names of employees that have left the hospital are send periodically to the IT department, in order to block their user account. One hospital has introduced a system where user accounts are blocked automatically when the leave date is entered in the HR system.

While this system seems to work, many hospitals struggle with employees without a salary that are leaving the organization, such as contractors, external medical specialists and volunteers. One hospital proposed a system were the user accounts are verified with the responsible managers on a regularly basis, but it not known yet whether this method is effective.

In many hospitals, user rights are based on the job function and the department of a user. Most hospitals do restrict access to information which are not deemed relevant for certain groups of employees, or access to this information is logged specifically (such as the escalation procedure for electronic patient records).

8.1.7.1 Authentication

One aspect of access control is authentication. Users are in most hospitals authenticated by entering a username or password. Most hospitals enforce minimum requirements for the passwords, such as a minimum length or period changes. These requirements are usually based on the NEN standard. Only in a few cases the password requirements were not technically enforced (adherence to the password policy is avoidable by users in these hospitals).

Some hospitals employ smartcards for authentication of employees. This is an effective and secure technique, but various respondents have indicated that it is also relatively costly.

Using common accounts for groups of employees (group accounts) is a common practice among Dutch hospitals, although various hospitals are currently phasing out these type of accounts (or they have already abandoned them). Shared, non-personal accounts may have an useful function and do not necessarily reduce information security: for instance, in an operating room, physical access is already difficult and timely access to the hospital's information systems is crucial. Employing a group account that has limited permissions and is restricted to the physical OR workstation can be useful. Often, access to patient information requires a personal user account and group accounts provide only access to the operating system and common documents.

Some hospitals use group accounts to give multiple employees access to a computer. There are few hospitals which do not provide personal user accounts to employees. This is problematic because passwords needs to be shared among a large group of users (with risk of unintentional disclosure) and access to information cannot be traced back to an individual, making it more difficult to make users responsible for their actions.

8.1.8 Information systems acquisition, development and maintenance

Objective: To ensure that security is an integral part of information systems.

Multiple hospitals have adjusted the purchasing conditions: when new systems are acquired, the system has to conform to the hospital's security policy or the system needs to be adjusted so that it conforms to this policy. In some hospitals, the IT department now refuses to connect a new system if it is not declared to conform to the security requirements.

However, there are also hospitals known in this study where information security is not yet an integral part of the acquisition of new systems. Sometimes, new systems are acquired which do not conform to the requirements, yet these systems are still connected to other systems and being used. This seems to be related to a lack of support by higher management levels.

8.1.9 Information security incident management

Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

The view that is distilled from the hospitals is somewhat varying. Multiple hospitals enable employees to report insecure situations, but the approach is different among these hospitals. Some hospitals have linked reporting information security incidents to a system where employees can report incidents regarding patient safety. Others have a separate reporting method (e.g., a special email address). Yet other hospitals link the incident report procedure to the support system which is already being used by the IT department (for instance to request new accounts or to report malfunctioning printers).

The first two methods both seem to work well to record security incidents. When the incident reporting procedure is linked to the IT department's support system, it is observed that the security officers feel that there are less security reports (compared to the answers of their colleagues).

8.1.10 Business continuity management

Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

Some hospitals take an integral approach and integrate information security in their overall business continuity management. Information security is placed in context with the primary activities of the organization. This approach is mainly manifested in the (quality of the) integral risk analysis and the emergency procedure for information security incidents: some hospitals have mitigated the risks of IT disruptions for the primary healthcare process, where other hospitals mainly focus on the standards and on the more technical and practical aspects of information security.

8.1.11 Compliancy with legal requirements

Objective: To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.

The security standard which has been implemented by all Dutch hospitals is already mandated by Dutch laws and compliancy is verified by the Dutch Healthcare Inspectorate and the Data Protection Authority. It is unknown if and how hospitals comply with other legal requirements.

8.2 Observations

When looking at the previous section (the structured analysis), it is also possible to make some observations on a higher level. The categories from the ISO standard that were used are still at a rather detailed level, this section aims to exceed that level. This section also tries to accept (or reject) the hypotheses that were defined in chapter 5, and to answer the research questions defined in chapter 3. The hypotheses and research questions will act as a guide for this section. Some general observations will also be made.

When possible, the observations described here will refer to the triad confidentiality, integrity and availability (the CIA triad) that was introduced in section 4.1.

8.2.1 Need to improve information security

The second hypothesis states: 'It is necessary to increase the level of information security.' Based on the results and the analysis in the previous section, it is possible to say something about this. When looking at the actions that have been taken by most hospitals, it is clear that there has been some improvement in the level of information security: many hospitals have introduced security policies, many hospitals are enforcing strong passwords and are taking other measures to increase the level of information security. However, it is important to realize that many hospitals have taken these actions only because of the interest that has been paid to the subject by the Dutch Healthcare Inspectorate and the Data Protection Authority. Both in 2004 and in 2008, information security was not sufficient according to earlier research and some severe pressure was needed to stimulate hospitals to take action. It is therefore the question whether hospitals will still improve information security when there is no pressure from the authorities.

Is it necessary to improve information security? One could say that a majority of the hospitals received a sufficient score for the mandatory external audit. However, this score is a minimum score and the audit was based on the NVZ regulations – a rather limited subset of the NEN 7510 standard. Hospitals were already in 2010 required to comply with this subset of requirements, but a majority of the hospitals was not able to comply at that time and had to be audited again in 2011. When keeping this in mind, complying to the NVZ regulations is not rather ambitious. The fact that there are still multiple hospitals that have received an insufficient score in 2011 contributes to the idea that information security still needs to be improved in some hospitals.

Another outcome of this research is that roughly one third of the hospitals does not have a sufficient risk analysis. This means that these hospitals have taken various security measures, but that these security measures are not the result of a risk analysis. The security measures might be sufficient, but it is difficult to know this for sure: it might be possible that certain treats are not mitigated by taking security measures.

8.2.2 Compliancy

The previous section already discussed compliancy to the NEN 7510 standard. Based on the results of this research, a majority of the hospitals comply with the NVZ regulations, a subset of the NEN 7510 standard. As said earlier, there are hospitals which do not even comply with the NVZ regulations. The hypothesis 'Information security within Dutch hospitals does not comply with the mandatory standards' cannot be rejected, because there are still hospitals with an insufficient level of information security.

Another observation that can be made is that two different ways can be distinguished in how hospitals implement information security. One group of hospitals take a risk-based approach, where information security risks are analyzed and security measures are taken based on existing risks. The other group of hospitals take a rather ad-hoc approach: security measures are implemented because these are prescribed by the security standards.

8.2.3 Problems with improving information security

An important aspect of this research was which problems hospitals face with improving information security. It was expected that there is some sort of conflict between common practice in hospitals and protecting information with security measures.

Based on the results of the research, there seems indeed to be a conflict between common practice in hospitals and effective security measures. Some of these problems will be discussed. However, for many of these problems, there are other hospitals which have found an effective solution to these problems – many of these problems can be solved by acquiring new technology, by modifying processes, or by other measures. These are further described under 'Best practices'.

Various problems are related to the conflict between the desire for rapid, unrestricted access to medical information (which improves patient safety, because relevant information is known), and the desire to restrict access to sensitive information (which improves a patient's privacy). It is not always possible to harmonize these desires: providing unrestricted access to medical information means that concessions are made to the protection of this information. In terms of the CIA triad, this is a typical conflict between maintaining confidentiality (restricting access to information) and availability (ensuring that information is available).

It is important to consider the context per case. For instance, in an OR, physical access is usually already restricted, and accessibility and availability of medical information is far more important. In a policlinic, physical access is usually not restricted and quick access to medical information is less important for patient safety. Protecting access to medical information is far more important instead, because policlinics can be publicly accessed.
When taking such differences in consideration, it is important to determine the risk of a specific location or specific system. This may lead to different security requirements throughout the hospital: workstations on a policlinic can be automatically locked for instance, while computers in an operating room are never locked. Each hospital should make such decisions in order to take the most effective security measures, without harming patients' interests.

An important factor that could be distinguished from this research is how mature an hospital can be considered on information technology. Hospitals that mainly use electronic patient records (instead of paper patient records) seem to have a better understanding of information security risks, and these hospitals have usually taken more severe security measures to protect this information. Furthermore, various respondents indicated that the maturity of a hospital's IT department is an important factor for the information security level. Some of the problems

found in this study indeed seem to be related to the professionalism and maturity of an IT department. Some hospitals, for example, do not know which applications exist or who administers such applications. This makes it difficult to secure these applications. Another example is the fact that some hospitals impose no restrictions on workstations: these hospitals allow employees to install their own software (risk of viruses) or modify security settings (such as increasing timeouts, not technically enforcing periodic password changes). Both examples are dangerous to information security.
On the other hand, there are also examples of hospitals in this study where the problems described above do not apply. These hospitals have a complete registration of installed applications and usage of these applications, employees do not have permission to alter computer settings or to install unauthorized software, et cetera.

Related to the maturity of an hospital on information technology, is the seriousness and thoroughness of an hospital when introducing information security measures. Some hospitals have taken information security more serious than others. Especially the role of the management and the board of directors is important: when the board of directors support information security goals, it is easier to introduce security measures, even when these security measures are unpopular or when substantial financial investments are required. Some boards see information security as an unwelcome topic to which they only have to pay attention because authorities demand hospitals to take some (minimum) measures. The security measures taken by these hospitals are often less thorough and less effective for information security, because there is no management support for more demanding security measures. It seems therefore that management support is crucial for effective information security.

It is observed that most hospitals have taken security measures to protect loss of information in cases of disruptions or power outages, such as backup procedures and emergency power supplies. The amount of hospitals that have taken security measures to make critical information available to medical workers in case of disruptions is notably smaller. While there are various options to make this information available (see also the best practices further on), a substantial amount of the hospitals have taken no security measures. This is not always a problem when most information is recorded in a paper medical record, but as more and more information is being stored in electronic systems, this problem and the consequences of it become more and more important.
When considering the CIA triad again, it can be observed that many hospitals have taken security measures to ensure that information stored in electronic systems is preserved (addressing the integrity aspect). The availability aspect, on the other hand, is often not addressed completely.

There are some problems which need to be addressed by the healthcare sector in general. Especially exchange of medical information (between healthcare organizations) is a topic where technical standards are required to ensure that all healthcare organizations are able to exchange information in a secure manner. For instance, secure e-mail is only useful when both the sending and the receiving party can use the same encryption standard.

An important observation in the validation study is that many problems are shared among hospitals. There are few problems that are specific to a single hospital; in most cases, the problem is shared with other hospitals that are comparable in some aspect: some problems are typical for small hospitals (such as limited resources), other problems are typical for hospitals which are fully switched to electronic patient records (such as providing timely access in case of disruption), etc.

8.2.4 Best practices

One of the research questions was whether it is possible to distinguish common patterns and best practices. This section will provide some best practices that were found during the research: best practices are successful approaches to mitigate problems that were seen in other hospitals.

One complaint that was expressed by many respondents is that it often takes a long time to log in into Windows (the operating system that was used by all hospitals in this study). In some cases, logging in could take between three and five minutes, which is indeed quite long and which makes it quite time-consuming to switch between users – which is why nursing personnel often uses an account of someone who is already logged in. But there are also hospitals which have found a practical solution to this problem: switching to a 'thin clients system' has reduced the time to log in significantly, and by employing RFID cards to log in (instead of using a username and password), it is easy for employees to switch to their personal account. Multiple hospitals have employed this technique and are satisfied about it.

Another problem which was experienced by multiple hospitals was that accounts of employees that are no longer employed for the organization are not blocked: the IT department is not aware of employees leaving the organization, and as such, accounts are often left in use. However, multiple hospitals have found a solution to this problem: the systems of the HR department (where a discharge is registered) are linked to a system which creates and deletes accounts automatically. This relieves the burden on the IT support desk, but also ensures that accounts are deleted timely. This practice does not provide a solution for employees or volunteers that are not registered in the HR system, however (e.g. unpaid interns or external employees). One hospital is considering a system where such accounts are regularly verified (and need to be confirmed) by the responsible manager. It is not known yet whether this system functions well.

Various hospitals have taken measures to ensure that electronic patient records are also accessible in case of a network disruption. Two important measures can be identified as 'best practice': the first one is the establishment of a central read-only copy of the EPR system, which can be consulted when the main production system is not available. This central read-only copy is useful when the primary network infrastructure is working, but when there are disruptions to the EPR system – e.g., problems with the servers or when an upgrade is performed. This system depends however on the correct functioning of main network components.
Another technique which is seen is that hospitals have special 'emergency computers'. These computers – sometimes mobile laptops, sometimes fixed workstations – have an own power supply for several hours and they contain a recent copy of the electronic patient records. Because the system does not depend on other network components, patient records are always accessible.

Another important best practice that follows from the research is that it is important to record exceptions to security policies. This makes it possible to verify regularly whether these exceptions are required, what risks are involved and what measures are taken to mitigate such risks. Recording and justifying exceptions is required by the standards (as part of an information security management system), but not every hospital already employs an ISMS.

Taking an integral approach is a practice that is employed by multiple hospitals. 'Integral approach' means in this case that not only specific information security risks are considered, but all kinds of treats to the primary processes of the hospital. This approach makes it better possible to place information security in context.

8.2.5 Roles of each party

It is important to consider which external parties have a role within the process of hospital information security. Each of these parties has their own interests.

Besides the hospital itself, the following parties can be distinguished:

- Dutch Healthcare Inspectorate (IGZ)
- Data Protection Authority (CBP)
- Association of Dutch Hospitals (NVZ)
- Auditors
- Suppliers

As can be seen, various parties are involved. The role of the Healthcare Inspectorate and the Data Protection Authority are clear: these two authorities look after the compliance to laws and governmental regulations. The Healthcare Inspectorate has special attention for the quality of healthcare, including the quality and availability of medical information. The Data Protection Authority mainly focuses on maintaining privacy for patients.

The Association of Dutch Hospitals can be seen as a representative of all Dutch hospitals. It represents the interests of their members. As such, it negotiated in 2009 about the minimum security requirements for hospitals, ensuring that these requirements were not too strict.

These parties have different interests. While the authorities want to ensure that each hospital complies with legal requirements and industry standards, the association of hospitals rather would like to weaken the regulatory burden on hospitals. In the past years, many improvements in information security have been fuelled by the pressure of the authorities and not by hospitals themselves or by the association that represents them.

Another important party in process of information security are external auditors. These external auditors analyze whether an hospital complies to the required regulations and hospitals can use such an analysis in turn to prove their compliance to the Healthcare Inspectorate. While this seems like an effective way to verify whether the level of information security in an hospital complies to the minimal requirements, this also brings a risk: the result of an external audit is important for an hospital and it may initiate action from the authorities. The result of an audit is therefore of many value to an hospital. Auditing organizations have a rather disputable relationship with hospitals: they are selected and paid by the hospital to perform an audit. As such, these organizations depend on the hospitals. Another problem that was suggested by respondents in the validation study is the quality of the auditing organizations: some of the organizations have little experience with information security audits and the quality of these audits was experienced as poor. There are no formal requirements to perform a NEN 7510 audit and the standard is not associated with accreditation organizations, which means that there is no independent supervision on the auditing organizations. Combined with the fact that auditing organizations are selected and paid by the hospitals that ought to be audited, means that there is a risk that the audits are biased. While there was in this study no concrete indication that audit reports were biased, the risk for this is inherent to the system that is used.

8.3 Summary

This chapter analyzed the results of both the case study and the validation study. The results of both studies were to a large extent comparable: both the process to improve information security was often similar in other hospitals, as well as problems that prevent this

improvement. However, there were also various solutions found to these problems – ‘best practices’ that are used by one or more hospitals to mitigate security risks or to find a good balance between effective security measures and a workable environment.

The next and final chapter presents the conclusions of this study. This chapter also answers the research questions posed in chapter 3.

9. Conclusions and future work

This chapter concludes the results of the study and the analysis made in the previous chapter. The research questions are answered in this chapter.

For reference, the research questions defined in chapter 3 are repeated here.

The main research question was:
How can hospitals improve information security successfully and in compliance with the standards?

And the following sub questions were defined:

1. How do hospitals currently implement security regulations?
2. Do hospitals encounter problems while improving information security?
   If so, what are these problems?
3. Is it possible to distinguish a common pattern or 'best practices'?
4. How do hospitals comply with the standards?

The sub questions will be answered first, after which then the main research question shall be answered.

9.1 Sub research questions

1. How do hospitals currently implement security regulations?

For the first research question, it has become clear how hospitals currently implement security regulations. Different approaches are applied, and the most common are a risk-based approach and a regulations-based approach. The first one implies that hospitals analyze information security risks and decide – based on the analysis – which risks are unacceptable and should be mitigated by taking security measures. These security measures can be both technical and organizational measures. Risks can also be prioritized using this approach. The other approach follows more strictly specific requirements outlined in security standards, such as technical requirements.

The method which is used by hospitals to implement such measures is different: some hospitals have a working group where representatives of various departments discuss security measures, in other hospitals, there is a single information security officer who is responsible for initiating actions (and the security officer contacts other departments when needed). There is no indication that one method should be preferred over the other method; both approaches seem to work well.

Is there a need to improve information security? Based on the analysis, it can be said that there are still hospitals which do not comply with basis security requirements. Moreover, the baseline is only a selection of security measures, and it can be questioned whether this selection is not too limited – it was introduced to decrease the amount of security requirements for hospitals. A revised version of the NEN 7510 standard has been introduced recently, which contains various changes with respect to the old standard.

2. Do hospitals encounter problems while improving information security?

Based on the results of this research, it has become clear that hospitals indeed face various problems while improving information security.

Various problems originate from the problem to decide which is more important, restricting access to information (to comply with security regulations) or to provide unrestricted and

rapid access to information (for patient safety and effective healthcare). However, there is not a general decision that can be made: it is different per case which interest prevalent over the other. In an OR, for example, it is clear that rapid access prevalent over strict security regulations preventing access to patient information. But in other cases, the situation is less clear. The hospital should decide per situation which security measures can (or should) be taken, in order to maximize information security and to protect privacy of patients as good as possible. Patient safety should never be compromised: when rapid access to information is needed, hospitals should not impose security measures which take more time. On the other hand, restricting access does not necessarily imply that accessing information consumes more time. There are various examples in this study where access to information is protected while it is still possible to access this information quickly. Such solutions may require substantial investments, but it makes it possible to address both the accessibility issue as well as security issues.

The maturity of the hospital's IT department and how the hospital treats information technology seems to be an important requirement to improve information security: for an hospital with an immature IT department or with an outdated vision on information technology it is far more difficult to establish effective information security.

One problem was found that is very difficult to solve for a single hospital: to secure exchange of medical information between healthcare providers, cooperation is required from other healthcare providers as well. The association of Dutch hospitals has started to discuss a solution for all Dutch hospitals, but it is important to realize that – besides hospitals – also other healthcare providers should implement this system to secure their communications. A more sector-wide approach would therefore be useful. A national system to electronically exchange patient records is currently being introduced within the Netherlands (albeit with delays and much criticism), but it would be useful to pay attention to other forms of information exchange as well – primary communication methods such as fax, e-mail or postal mail are usually not (or cannot be) secured.

3. Is it possible to distinguish a common pattern or 'best practices'?

It was possible to distinguish multiple best practices for problems which were found to be problematic for other hospitals. Sometimes the investments for these solutions are simply too high for an hospital; the hospital cannot or does not want to invest in these solutions. But in other cases, hospitals are simply not aware of best practices applied by other hospitals.

The following best practices were found:

- Using thin clients and terminal servers to improve login times and to fasten user switches;
- Using RFID badges or smartcards to reduce the time needed to authenticate;
- Integrating network accounts to other systems, which simplifies account administration and enforces password policies also for other applications;
- Integrating the HR system with the provisioning system for user accounts, accounts of employees leaving the hospital are automatically disabled;
- Maintaining a read-only version of the EPR database which can be consulted in case of disruptions or planned maintenance;
- Employing emergency workstations with local copies of the EPR database to provide electronic patient records in the case of network disruptions;
- Regular print-outs of pharmacy orders, medical records and other critical information to ensure healthcare when access to electronic systems is not possible;

- Recording and periodical verification of exceptions to security policies, to ensure that these exceptions are still required;
- Taking an integral approach instead of an approach solely focused on information security, to maximize the effectiveness of security measures.

4. How do hospitals comply with the standards?

As already discussed in the first subsection, most hospitals now do comply with the requirements of the Dutch Healthcare Inspectorate: they have a sufficient score for the minimum requirements. However, these audits are based on the NVZ regulations, a subset of the complete regulation. One can therefore not expect that most hospitals comply with the more extensive NEN 7510 standard. Only one hospital in this study was certified against the NEN 7510 standard, which means that all obligatory controls were implemented. For all other hospitals, it remains unclear whether they comply with all required elements in the NEN 7510 standard.

Does the NEN 7510 standard suffice as a minimum requirement for information security? Various hospitals complained that it is difficult to comply with all elements of the NEN 7510 standard, which was also the reason to construct the NVZ regulations as a subset of required elements. The NVZ regulations are quite restricted in usefulness and applicability: the regulations explicitly discourage to use the regulations as a benchmark, and the regulations do not cover all aspects that are important for information security. However, the NEN 7510 standard has been completely revised in 2011 and there have been various improvements; the standard is also compatible with international standards.

Most issues that were found during this research were conflicts between the confidentiality aspect and the availability aspect. While the NEN 7510 standard pays attention to this topic, much is left to the judgment of an hospital (with the mandatory risk analysis) and it is up to an hospital to decide – per situation – which aspects is more prevalent.

9.2 Main research question

How can hospitals improve information security successfully and in compliance with the standards?

Can hospitals improve information security, and how? This was a central question throughout this research. In the previous sections, various recommendations have been made how hospitals can efficiently improve information security, based on successful practices found at other hospitals. It is important to realize what risks are threatening hospitals. Not only hospitals that are fully transformed to electronic patient records are prone to information security risks: all hospitals may have severe problems with their primary healthcare process if there are no adequate security measures taken.

An important conclusion is that it is important to consider information security seriously. When the upper management of an hospital fails to do so, it is seen that it is difficult to introduce security measures and to justify investments for information security. Furthermore, it is important to make it clear who is responsible for which aspect of information security. In most cases, a single security officer is simply not able to oversee everything – he or she is therefore dependent on other employees and departments within his organization. A supportive upper management is therefore important to realize information security objectives.

Multiple problems have been found which are common among Dutch hospitals. Some of these problems require collaboration with other hospitals. Especially when communication

with other healthcare providers is involved, it is necessary to agree on secure methods to exchange patient information. It is important to ensure that such exchange methods are used by all hospitals, otherwise there is still exchange of information via insecure ways.

The answer to this question can be summarized as: take information security seriously, and solve problems together. Only by addressing the subject in a serious manner, it is possible to remain compliant with the standards for information security, and by solving problems together with other hospitals, knowledge can be shared and shared problems can be solved.

9.3 Future work

This study has taken an explorative approach to research how Dutch hospitals improve information security. While this study has found many insights in this process, it is difficult to quantify the results: this was not the nature of the study, and the research method was tailored towards finding as much information as possible instead of comparing information security levels of hospitals. However, it would be useful to have more quantitative data: a future study could take a quantitative method to verify the results found in this study.

A related issue is that this research method makes it difficult to benchmark hospitals. Effective solutions for problems were identified, but using the results of this study, it is difficult to say whether a particular hospital has a higher level of information security compared to another hospital. There are of course indicators for the information security level – for instance, scores of audits performed by external parties – but these indicators do not address all aspects of information security and are usually also not specifically designed for benchmark purposes. The development of a tool for benchmarking information security in hospitals would be a useful future work: this makes it possible to compare hospitals to each other and to see which hospitals have implemented effective security measures. One of the requirements for a benchmark tool would be that it addresses all aspects of information security. The aspects confidentiality, integrity and availability are useful domains to structure benchmark results: these three aspects cover the most important aspects of information security. Another important requirement of a benchmark tool is that care should be paid to the weight of score elements. The scoring system that has been used until now allows compensating insufficient scores with outstanding scores for other elements; a benchmark tool should compensate for that. Furthermore, it is important that a benchmark tool should determine an hospital's information security level by looking at technical aspects as well as organizational aspects.

Another recommendation of this study is to investigate the current system of auditing information security within an hospital. As pointed out in section 8.2.5, this system provides room for biased audit results and there is no warranty that auditors are fully objective. A revision of this system should pay attention to the relationship between auditing organizations, hospitals (which are now paying customers of the auditing organizations) and independent supervisors (such as accreditation bodies and the Dutch healthcare inspectorate).

10.Literature

Anderson, J. M. (2003). Why we need a new definition of information security. *Computers & Security*, *22* (4), 308-313.

Automatisering Gids (2011). Zorgverzekeraars redden EPD-infrastructuur. Retrieved on December 12, 2011 from http://www.automatiseringgids.nl/nieuws/2011/49/zorgverzekeraars-redden-epd-infrastructuur

Boone, Jan, Douven, Rudy, Droge, Carline and Mosca, Ilaria, Health Insurance Competition: The Effect of Group Contracts (May 19, 2010). TILEC Discussion Paper No. 2010-040. Available at SSRN: http://ssrn.com/abstract=1618764

College Bescherming Persoonsgegevens & Inspectie voor de Gezondheidszorg (2008). Informatiebeveiliging in ziekenhuizen voldoet niet aan de norm. Den Haag, NL: Inspectie voor de Gezondheidszorg. Retrieved May 5, 2011 from http://www.cbpweb.nl/downloads_rapporten/rap_2008_informatiebeveiliging_ziekenhuizen.pdf

Dutch Hospital Data (2009). Kengetallen Nederlandse ziekenhuis 2009. Retrieved from http://www.dutchhospitaldata.nl/Bestanden/Documenten/Kengetallen_Nederlandse_Ziekenhuizen_2009.pdf

Eerste Kamer der Staten-Generaal (2011). Stand van zaken digitale gegevensuitwisseling in de zorg na aanvaarding van de motie-Mulder: letter from the Dutch Senate to the Minister of Health, Welfare and Sport about the state of medical information exchange in the healthcare sector. Retrieved on December 12, 2011 from http://www.eerstekamer.nl/behandeling/20111129/brief_van_de_commissie_voor_vws/info

Hingstman, L., Kenens, R.J. (2009). Cijfers uit de registratie van huisartsen: peiling 2009. Utrecht: NIVEL. Retrieved December 3, 2011 from http://www.nivel.nl/pdf/cijfers-uit-de-registratie-van-huisartsen-peiling-2009.pdf

Inspectie voor de Gezondheidszorg (2004). ICT in ziekenhuizen: beveiliging van informatie nog onvoldoende voor een betrouwbare papierloze patiëntenzorg. Den Haag, NL: Inspectie voor de Gezondheidszorg.

Inspectie voor de Gezondheidszorg (2011a). Enforcement measures: administrative measures. Retrieved December 9, 2011, from http://www.igz.nl/english/enforcement_measures/administrative_measures

Inspectie voor de Gezondheidszorg (2011a). Informatie-uitwisseling in de zorg: ICT lost knelpunten zonder standaardisatie van de informatieuitwisseling niet op. *Staat van de Gezondheidszorg* (ed. 2011). Utrecht: Inspectie voor de Gezondheidszorg.

Knottnerus, J. A. & ten Velden, G. H. (2007). Dutch Doctors and Their Patients — Effects of Health Care Reform in the Netherlands. *New England Journal of Medicine* **357** (24), 2424-2426. (DOI: 10.1056/NEJMp0707383.) Retrieved from http://www.nejm.org/doi/full/10.1056/NEJMp0707383.

Krens, R., Spruit, M., Urbanus, N. (2011). Information security in Health care: Evaluation with Health Professionals. Proceedings of the 4th International Conference on Health Informatics (HEALTHINF 2011), 26-29 January, 2011, Rome, Italy, pp. 61-69.

Maarse, H. & Ter Meulen, R. (2006). Consumer Choice in Dutch Health Insurance after Reform. *Health Care Analysis* **14**, 37-49. Retrieved from http://dx.doi.org/10.1007/s10728-006-0010-z.

Nederlandse Zorgautoriteit (2011). Marktscan Medisch specialistische zorg. Retrieved from http://www.nza.nl/104107/105773/Marktscan_medisch_specialistische_zorg_2011.pdf.

NRC Handelsblad (2011). Elektronisch patiëntendossier komt er toch. Retrieved from http://www.nrc.nl/nieuws/2011/12/08/elektronisch-patientendossier-komt-er-toch/

Peltier, T. (2001). *Information Security Risk Analysis.* (1st ed.). (p. 266). Boca Raton, FL, USA: Auerbach Publications.

Pfleeger, C. P., & Pfleeger, S. L. (2003). *Security in Computing.* (3rd ed.). (pp. 29-30). Upper Saddle River, NJ, USA: Prentice Hall.

Schut, F. T. & Van de Ven, W. P. M. M. (2005). Rationing and competition in the Dutch health-care system. *Health Economics* **14** (S1), S59--S74. (DOI: 10.1002/hec.1036.) Retrieved from http://dx.doi.org/10.1002/hec.1036.

Siponen, M.T. (2005). Analysis of modern IS security development approaches: towards the next generation of

social and adaptable ISS methods. *Information and Organization, 15* (4), 339-375.

Vesseur, J. (2011). *Resultaten audits NEN 7510*. Presentation of June 22, 2011 at the NVZ association of Dutch Hospitals.

Webwereld (2011a). Senaat blokkeert nieuwe voorstel voor EPD. Retrieved from http://webwereld.nl/nieuws/108724/senaat-blokkeert-nieuwe-voorstel-voor-epd.html

Webwereld (2011b). Toch miljoenen van minister voor privaat EPD. Retrieved on December 12, 2011 from http://webwereld.nl/nieuws/108838/toch-miljoenen-van-minister-voor-privaat-epd.html

11. Appendixes

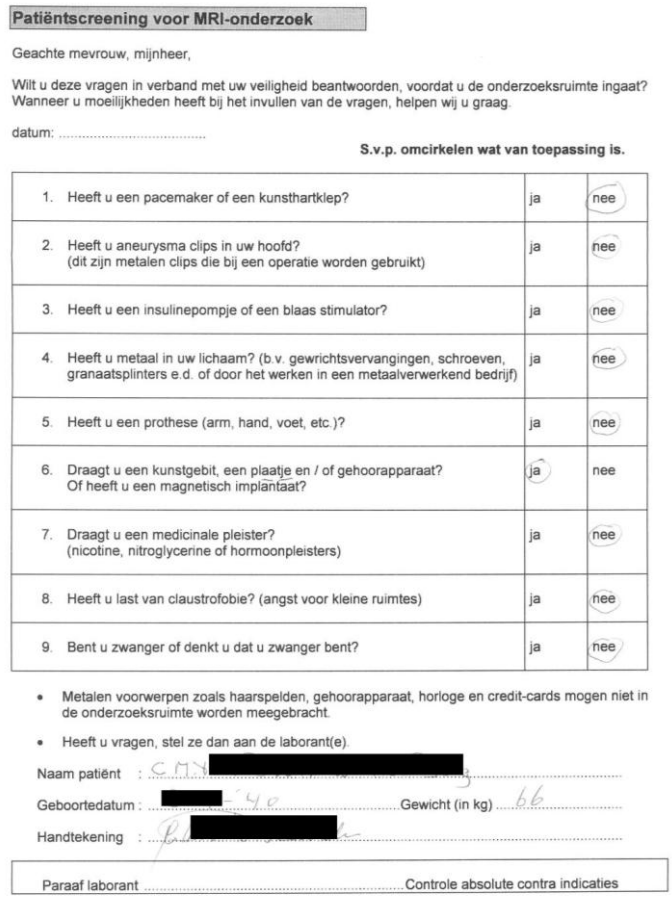
Appendix A: Interview format case study

Each interview was extended with questions based on the job of the respondent and his or her place within the organization. The questions below were asked independently of this.

1. Introduction to the research
2. What is your role/your department's role in information security?
    a. Responsibilities
    b. Authorities
3. Which measures did you or did your department take?
4. Which measures are you aware of that have been taken by others?
5. Which problems did you encounter while improving information security?
6. How could these problems be solved? Or were you able to find a solution for these problems?
7. How should the hospital deal with information security in the future?
8. Is the communication about information security good enough?
9. Are there any other remarks you would like to make about information security?

Appendix B: Documents found during observation

All these documents were found during an observation at the radiology department. Some documents have been partly censored to protect the privacy of patients.



Patiëntscreening voor MRI-onderzoek

Geachte mevrouw, mijnheer,

Wilt u deze vragen in verband met uw veiligheid beantwoorden, voordat u de onderzoeksruimte ingaat? Wanneer u moeilijkheden heeft bij het invullen van de vragen, helpen wij u graag.

datum: .....

S.v.p. omcirkelen wat van toepassing is.

1. Heeft u een pacemaker of een kunsthartklep?	ja	(nee)
2. Heeft u aneurysma clips in uw hoofd? (dit zijn metalen clips die bij een operatie worden gebruikt)	ja	(nee)
3. Heeft u een insulinepompje of een blaas stimulator?	ja	(nee)
4. Heeft u metaal in uw lichaam? (b.v. gewrichtsvervangingen, schroeven, granaatsplinters e.d. of door het werken in een metaalverwerkend bedrijf)	ja	(nee)
5. Heeft u een prothese (arm, hand, voet, etc.)?	ja	(nee)
6. Draagt u een kunstgebit, een plaatje en / of gehoorapparaat? Of heeft u een magnetisch implantaat?	(ja)	nee
7. Draagt u een medicinale pleister? (nicotine, nitroglycerine of hormoonpleisters)	ja	(nee)
8. Heeft u last van claustrofobie? (angst voor kleine ruimtes)	ja	(nee)
9. Bent u zwanger of denkt u dat u zwanger bent?	ja	(nee)

- Metalen voorwerpen zoals haarspelden, gehoorapparaat, horloge en credit-cards mogen niet in de onderzoeksruimte worden meegebracht.
- Heeft u vragen, stel ze dan aan de laborant(e).

Naam patiënt : C M [redacted]

Geboortedatum : [redacted] 40 Gewicht (in kg) 66

Handtekening : [redacted]

Paraaf laborant ..... Controle absolute contra indicaties

Standard questionnaire for patients before entering a MRI scan.

The form shows a patient's name, date of birth, weight, a signature, and a list of 9 medical questions (such as: 'Do you have a pacemaker?' or 'Do you suffer from claustrophobia?')

A staple of more than 30 forms was found in a paper recycle container.

secr.neurochirurgie 27/07/11 14:06

Medisch Spectrum Twente
Poli 14a Anesthesiologie
Preoperatieve-screening & Pijnpoli
Postbus 50000
7500 KA Enschede
Tel: 053-4873060
Fax: 053-4873093

[redacted] SCHEDE 053-47[redacted] MENZIS

(afdruk pons/sticker)

Patiëntenverklaring anesthesiologie

Hierbij geef ik toestemming aan de polikliniek anesthesiologie van het MST om medische gegevens op te vragen bij:

Aanvraag MRI + Röntgen
Sint Maartenskliniek Woerden.

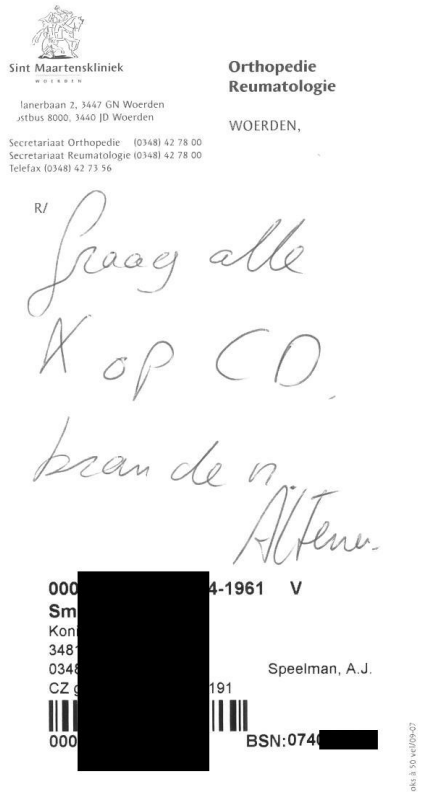
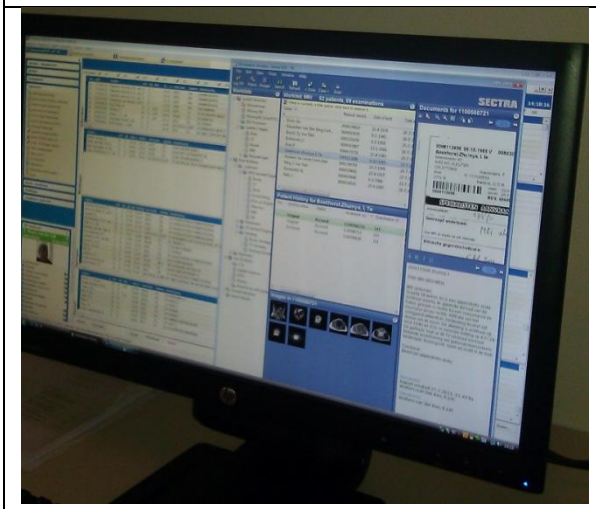
Enschede, 27-4-11

Handtekening: [redacted]

Hofpoort Ziekenhuis
Fax Radiologie
0348-427374

Approval of a patient to another hospital to request patient records from the Zuwe Hofpoort hospital. In the upper right corner of the page, a copy of the patient's hospital identification card.

The card shows the patient's name, address, social security number, telephone number, insurer and insurance number.

	This is a note written by a medical specialist, with a request to burn some pictures to a CD-R disc. In the lower part of the request, a sticker with identifies the patient is attached. The sticker shows the patient's name, address, social security number, telephone number, insurer and insurance number.
	Sign providing the login credentials for a group account for the radiology department (username and password). Literal translation: *Warning: All computers have Windows Vista now. Passwords have been changed because of that.* *For the department account, the password is: …* *(username, password and the password spelled out)*
	Unlocked computer that gave access to the hospital information system. The room where this computer was located could be used for more than 15 minutes without being interrupted.

Appendix C: Interview statements (case study)

General statements

Statement	Count	Percentage
A change of culture is required	4	7,41%
Each department implements the security policy in its own way	5	9,26%
Reminders at the workplace will not work	1	1,85%
Improving patient safety is much easier	1	1,85%
Access to medical records is logged, but not checked	2	3,70%
Hospitals have to work more efficiently, more market forces	1	1,85%
Progress is slowly visible	6	11,11%
The hospital is not an early adaptor; only proven software is used	1	1,85%
Healthcare department are responsible for an own emergency plan	1	1,85%
There is no special budget for information security	10	18,52%
Software suppliers maintain their own software	1	1,85%
Information security is also for other hospitals a problem	2	3,70%
Information security should be as easy-to-use as possible	1	1,85%
Businesses are much stricter on information security than hospitals	1	1,85%
The previous audit was one year too early	1	1,85%
My own department handles information security quite well	1	1,85%
My department works digitally to quite an extent	3	5,56%
Rooms are always occupied	2	3,70%
Rooms are always locked when not occupied	2	3,70%
The hospital information system provides advantages over paper records	1	1,85%
Senior management and the Board of Directors are responsible for information security	2	3,70%
Incomplete or incorrect information in a patient record is not always a problem	1	1,85%
Hospitals use more and more information technology	1	1,85%
The size of an hospital is an important factor for information security	1	1,85%
Many trust in colleagues and the hospital itself	2	3,70%
Total 25 unique statements	**54**	**100%**

Problems experienced with information security

Statement	Count	Percentage
Insufficient awareness	8	4,65%
Employees have more care for treating patients than for information security	9	5,23%
It takes a lot of effort to comply with the information security policy	8	4,65%
Patients don’t care for privacy either	1	0,58%
Employees look into medical records of colleagues	4	2,33%
Employees look into medical records of persons they don’t treat	4	2,33%

Statement	Count	Percentage
There are no sanctions against employees breaching the information security policy	10	5,81%
The government regulations are too strict	4	2,33%
Employees don't see the added value of information security	3	1,74%
Trustful atmosphere, no worries about abuse	3	1,74%
Little influence on medical specialists due to organizational structure (cooperations)	2	1,16%
Employees try to avoid the security restrictions	2	1,16%
Heavy burden on employees, no time for information security	3	1,74%
Users don't listen to IT advisories	1	0,58%
Employees have low computer proficiency	3	1,74%
Security measures are experienced as bureaucratic	6	3,49%
The configuration of Chipsoft is not restrictive enough	1	0,58%
There are workarounds in Chipsoft to circumvent security measures	2	1,16%
Security audits are time-consuming, but useful	2	1,16%
Employees don't see the confidentiality anymore of medical records	1	0,58%
There is a tension between a safe and a workable environment	5	2,91%
Some solutions are too costly (e.g. RFID, badge readers)	2	1,16%
Personnel retirement not always passed to IT; accounts are not deactivated	1	0,58%
Some employees very rarely present, some have a very long time off	1	0,58%
Employees do not realize the consequences of insecure behavior	1	0,58%
In an emergency case, users forget about information security	2	1,16%
Computer accounts are shared within a department	5	2,91%
Establishing support for information security is difficult	1	0,58%
Management does not look after employees (with regard to IS)	3	1,74%
Compromises are made with respect to information security, which do not adhere to the regulations	1	0,58%
Compromises are made with respect to information security, so a reasonable solution is chosen	1	0,58%
The Board of Directors does not co-operate	2	1,16%
There is not enough budget	1	0,58%
The Zuwe Hofpoort Hospital is a small hospital, not enough resources	1	0,58%
Small steps: always behind the latest regulations	1	0,58%
There are so many regulations to which hospitals have to comply	3	1,74%
E-mail is not secured	3	1,74%
Printouts are left at the printer	4	2,33%
Logging in takes too much time	6	3,49%
Switching users in Chipsoft takes too much time	2	1,16%
Users are often away from their computer, to walk around	3	1,74%
Users work in a secured room (badge reader/locked door)	3	1,74%
Computers are automatically locked too quickly	5	2,91%

Statement	Count	Percentage
The importance of privacy is understood	3	1,74%
Permission of patient to exchange information: cumbersome, not all hospitals ask permission	1	0,58%
It is not clear whether IT suppliers work on information security	3	1,74%
It is difficult for an hospital to judge itself on the effectiveness of information security	1	0,58%
Information security harms employees in their daily work	1	0,58%
There is not enough communication with end users	1	0,58%
Computer trainings are of an inadequate level	1	0,58%
Unclear and irrational distribution of rights	1	0,58%
There is no emergency plan or it is not known – ad-hoc procedures	2	1,16%
Specialists don't follow advices of their professional association	1	0,58%
Speech recognition makes mistakes sometimes	2	1,16%
Notes and paper medical records are left around	1	0,58%
Technical security is usually adequate	1	0,58%
Behavior is the most important problem	6	3,49%
Hospitals don't realize the risks of information technology	1	0,58%
Hospitals are too much focused on the NEN regulations	1	0,58%
Information technology does not always solve the problem of information exchange	1	0,58%
Information security should be intrinsic, focused from the patient	1	0,58%
Computers are not locked when users leave their computer	3	1,74%
The approach is reactive, not pro-active	1	0,58%
There have been many disruptions in the hospital's information system last month	2	1,16%
Sometimes computers are left unattended while the room is accessible	3	1,74%
Total 66 unique statements	**172**	**100%**

Security measures that have been taken

Statement	Count	Percentage
External and internal audits	5	5,32%
Foundation of a working group for information security	6	6,38%
Employees informed about information security condition in employment conditions	5	5,32%
Interviews about information security in the hospital's employees magazine	1	1,06%
Internal memos	4	4,26%
Technical changes (e.g., enforcing password changes)	8	8,51%
Security rounds	2	2,13%
Introduction program for new employees adjusted to include a section about information security	4	4,26%
Dual management: medical specialist and senior manager	1	1,06%
Ad-hoc sanctions for severe violations of the security policy	1	1,06%

Statement	Count	Percentage
Redundancy and mirroring of hospital servers	1	1,06%
Snapshot technology	1	1,06%
Daily backup on tape (stored locally)	1	1,06%
Weekly backup, stored externally	1	1,06%
Virus scanners, spam filters	1	1,06%
Lockdown of workstations: restrictions on USB ports, external media, etc.	3	3,19%
Virtualized applications	2	2,13%
Automatic login on some computers (operating rooms)	3	3,19%
Network divided in different segments (VLANs)	1	1,06%
Employees supported with new workstation configuration: brochures, assistance at the workplace, etc.	2	2,13%
Division of roles	2	2,13%
Contracts and conditions for suppliers	2	2,13%
Suppliers have limited permissions	1	1,06%
Phasing out shared accounts	1	1,06%
Specific configurations for some computers	1	1,06%
Risk analyses	2	2,13%
Using the same credentials for all systems, eliminating the need for multiple accounts/passwords	1	1,06%
Computer accounts linked to personnel badges	1	1,06%
Account request process improved	1	1,06%
Information system for job applicants: improved security	1	1,06%
There is a policy on using IT equipment	4	4,26%
Computer monitors mounted in such a way that patients cannot look at the screen	1	1,06%
Leaflets about information security spread among employees	3	3,19%
An emergency plan for IT malfunction is available	4	4,26%
Employees are not allowed to take medical records home	2	2,13%
Patients must give permission before information is exchanged	1	1,06%
Patient records are not exchanged with other healthcare providers anymore	1	1,06%
Employees point out non-locked workstations to colleagues	5	5,32%
Important or severe operations are always discussed with two specialists	1	1,06%
Often technical disruptions with the information systems	3	3,19%
Completeness of information	1	1,06%
Sanctions of the Dutch Data Protection authority	2	2,13%
Total 42 unique statements	**94**	**100%**

Proposals for improving information security

Statement	Count	Percentage
Active monitoring of Chipsoft log files	2	11,11%

Statement	Count	Percentage
Suggestion box (for suggestions on improving information security)	1	5,56%
Technical security measures should not be too severe	2	11,11%
Printing only with a personnel badge	1	5,56%
Introduction of a sanction policy	3	16,67%
General leaflet about information security	1	5,56%
Adding information security to the expedition part of the introduction program	1	5,56%
Video about quality and safety, with inclusion of information security	1	5,56%
Linking information security to carefulness and professionalism	1	5,56%
Sending a letter to employees about information security to their home address	1	5,56%
Additional confidentiality agreement to Chipsoft training	1	5,56%
Logging in with fingerprint instead of a password; saves time	1	5,56%
Approaching IS from patient safety instead from regulations	1	5,56%
Modifying Chipsoft to single authorization instead of switching user	1	5,56%
Total 14 unique statements	**18**	**100%**

Appendix D: Interview format validation study

1. Introduction to the research
2. Can you describe your hospital?
    a. What is the size of the hospital, etc.
    b. How far is it automated/digitized?
    c. Do you use an EPR?
3. How did the hospital score on the last external audit for information security?
    a. Which areas needed improvement?
    b. Is the general risk analysis found to be sufficient?
4. How is information security organized within your hospital?
    a. Which department or officer is responsible?
    b. To who does the security officer report?
    c. Is there a relation between the quality and safety policy of the hospital?
    d. Is there a working group (or similar structure) to take security measures? If so, what authorities does this working group have?
    e. Are there other departments involved?
    f. Do you use an information security management system (ISMS)?
    g. Is there a security policy defined and approved by the management?
    h. How is the policy evaluated? Are there structural tests, audits, mystery guests, … ?
5. Employees
    a. How are security measures communicated to employees?
    b. Are the employments conditions adjusted for information security/confidentiality? Do employees have to sign a non-disclosure agreement?
    c. Are these measures also taken for volunteers within the hospital?
    d. Are there ‘house rules’ for using information systems? Is it allowed to use information systems for private usage?
    e. What problems do you encounter with employees? (E.g., notes with passwords, borrowing accounts, etc.)
6. Computer accounts
    a. Does every have a personal user account?
    b. Are there shared (group) accounts? If so, what is the policy on these accounts?
    c. What is the procedure for creating a new account for new employees? And what happens with accounts belonging to employees that leave the organization?
    d. Is there a password policy and if so, is this technically enforced?
    e. Are accounts shared among employees?
    f. Is it possible to log in once to access all applications (single sign-on), or should users authenticate for every single application?
7. Security of workstations
    a. Are computers locked automatically? If so, after how many minutes?
    b. Do employees lock the computer when leaving their workplace?
    c. What permissions do users have on their workstation? Can they install applications?
    d. Can users use USB memory drives?
    e. Do you know what the average log-in time is?

8. Technical central security measures
    a. Does the hospital make a backup regularly?
    b. Is the network redundant?
    c. Is there an emergency power supply?
    d. Are there often disruptions in the hospital's information systems? If so, what is the impact of them?
9. Emergency procedures
    a. Are there emergency procedures for information security incidents?
    b. Are there specific emergency procedures for healthcare departments?
    c. Are all employees aware of the emergency procedure?
    d. What elements does the emergency procedure contain?
    e. Is the emergency procedure available off-line?
    f. Is the procedure tested?
10. Training and education of users
    a. Are most employees proficient with information technology?
    b. Does the hospital provide any training for employees with lacking computer proficiency?
11. Decentralized applications
    a. Are there known decentralized applications?
    b. Is there a policy on such applications?
    c. Are administrators of such applications aware of the security measures they should take?
    d. Do vendors allow to install virus scanners on medical devices? If not, did you mitigate risks from these devices and how?
12. Do you recognize the following observations?
    a. Personnel accessing medical records without permission and without medical need.
    b. High trust in colleagues and visitors, dependence on social control.
    c. Employees are unaware of information security risks.
    d. Security incidents are approached in a reactive manner: the hospital is not prepared beforehand and does not evaluate afterwards.
    e. Healthcare workers do not feel responsibility for information security.
    f. Medical specialists are stubborn and often do not feel the need for information security measures.
    g. Many information is exchanged via unsecure e-mail.
13. Have you seen problems with the integrity of information?
14. How are security incidents recorded?
    a. What type of system does the hospital use? Is it linked to another system?
    b. Are incidents evaluated, does the hospital learn from them? Are patterns recognized?
15. How is information exchanged; what security measures are taken?
16. Are there any other obstacles for effective information security? For example: financial problems, or problems with other departments that do not cooperate.
17. What do you think of the regulations? Are these sufficient? Is the approach right?

Appendix E: Interview statements (validation study)

Organization

Statement	Count	Percentage
There is a large working group for information security	4	23,5%
There is a small working group for information security	2	11,8%
There is no working group for information security	7	41,2%
Improving information security is seen as a project	2	11,8%
Improving information security is seen as a continuous process	6	35,3%
The board of directors is involved with information security	7	41,2%
The board of directors is not involved with information security	3	17,6%
There is a full-time security officer	10	58,8%
There is a part-time security officer (also devoted other tasks)	6	35,3%
Intensive cooperation with other hospitals for information security	6	35,3%
Information security is appointed to the quality/safety department	2	11,8%
Information security is appointed to job conditions	1	5,9%
Information security is appointed to internal auditing and control	1	5,9%
Information security is appointed to the IT department (operative/general IT)	1	5,9%
Information security is appointed to the IT department (policy/staff)	4	23,5%
Information security is appointed to innovation and organization	1	5,9%
Information security is appointed to the financial department	1	5,9%
Information security is appointed to a separate staff function	4	23,5%
The security officer has an advisory role	3	17,6%
Information security should be appointed to quality/safety (but it is not)	2	11,8%
Information security should be embedded in the hospital's quality/safety policy	4	23,5%
It is problematic to involve other departments	2	11,8%
It is not problematic to involve other departments	9	52,9%
It was a deliberate choice to appoint information security NOT to IT:	8	47,1%
- it encompasses more than only IT related issues	3	17,6%
- independence of ISO warranted	5	29,4%
- IT would focus too much on the technique	4	23,5%
- conflict of interests	4	23,5%
Deliberate choice to make IT responsible for information security:	2	11,8%
- because most security measures are technical measures	1	5,9%
- IT department is historically involved with this subject	1	5,9%
No conflict of interest because of position at IT department	3	17,6%
Responsibility for information security placed at line management	2	11,8%
There is a CERT to resolve technical treats	2	11,8%
Progress on information security is continuously monitored	2	11,8%
CBRN subsidy used to improve information security	4	23,5%
Mainly 'paper policy', little action	1	5,9%
Integral approach, not only focuses on information security	2	11,8%

Hospital organization

Statement	Count	Percentage

Small organization	9	52,9%
Large organization	7	41,2%
Informal organization	6	35,3%
Formal organization	4	23,5%
More than 1 location	9	52,9%
Share IT organization	2	11,8%
Completely indepedent hospital	13	76,5%
Part of a larger group (of hospitals)	7	41,2%
A HIS is used, but many paper records	11	64,7%
A HIS is used, partly paper records, partly electronic records	4	23,5%
Hospital only uses electronic records, no paper records anymore	1	5,9%
Goal to make hospital paperless in 2014	1	5,9%

History and earlier results

Statement	Count	Percentage
All clusters score a maturity level of 2 or higher	13	76,5%
Re-audit: score insufficient	3	17,6%
Integral risk analysis found to be sufficient	11	64,7%
Integral risk analysis found to be insufficient	5	29,4%
Working on new risk analysis	4	23,5%
Not yet started on new risk analysis	1	5,9%
Hospital visited in 2008 for joint CBP/IGZ research	3	17,6%
Hospital came in the news due to bad information security	2	11,8%
Hospital certified for information security (NEN 7510)	1	5,9%
Much was already in order, but not formalized	2	11,8%

Awareness and communication

Statement	Count	Percentage
Not or barely communicated about information security	1	5,9%
- that was a deliberate choice	1	5,9%
Extensive communication about information security	13	76,5%
Articles in hospital newsletter	6	35,3%
Articles in employees magazine	5	29,4%
Posters placed throughout the hospital	8	47,1%
Leaflets	8	47,1%
Plenary presentation for all employees	2	11,8%
Presentation for management	5	29,4%
Presentation during work meetings	2	11,8%
Reminders/notes at workplace to notify about insecure situations	4	23,5%
Notes at workplace to reward secure situations	3	17,6%
Wuppies at workplace to notify about insecure situations	1	5,9%
Video played to employees	7	41,2%
Placed video on intranet	2	11,8%
Text pages on intranet	3	17,6%
Flash game on intranet	3	17,6%

Made information security part of regular security rounds	8	47,1%
Internal audits/checkups	7	41,2%
External audits	7	41,2%
Penetration tests	1	5,9%
Mystery guest	3	17,6%
Phishing attempt to notify employees about phishing risks	1	5,9%
Continuous attention for information security	3	17,6%
There was a campaign, but it is over now	4	23,5%
Linked to other events	4	23,5%
Top-down communication: starting at the upper management, then further down	2	11,8%

Measures that have been taken

Statement	Count	Percentage
Each employee has a personal account	13	76,5%
Not a personal account for every employee	2	11,8%
There is a password policy	13	76,5%
Password policy is technically enforced	11	64,7%
Employees have to change passwords regularly	11	64,7%
There are complexity requirements	10	58,8%
There are no shared/group accounts in use	3	17,6%
There are some group accounts in use, becomes none	5	29,4%
There are some group accounts in use and it stays like that	6	35,3%
There are many group accounts in use	1	5,9%
Group accounts are chosen deliberately	9	52,9%
- group accounts used because switching users takes too much time	9	52,9%
Group accounts do not give access to EPRs (personal account must be used)	5	29,4%
Password reset: no check on identity	2	11,8%
Employees log in using RFID card	3	17,6%
Single sign-on: logged in in Windows means that user is logged in for applications	4	23,5%
No single sign-on: authentication separately per application	9	52,9%
Different passwords per application	10	58,8%
Passwords Windows/application are linked	1	5,9%
Accounts for HIS are personal	10	58,8%
Medical specialists can see all records	6	35,3%
All employees have access to all information	1	5,9%
Employees have only access to patients treated on their department	8	47,1%
There is a escalation procedure to access patient records without permission	7	41,2%
- Log files are verified periodically	2	11,8%
Interns receive a temporary account, must change passwords	1	5,9%

Measures that have been taken

Statement	Count	Percentage
Confidentiality clause in employment conditions	14	82,4%
Rules of the house modified or introduced	11	64,7%

Information security is discussed when hiring a new employee	2	11,8%
New employees are informed of information security policy	11	64,7%
Existing employees are informed about information security	6	35,3%
Employees in a trust function should provide certificate of good conduct	2	11,8%
There is a sanction policy	3	17,6%
IS abuse is sanctioned	10	58,8%
IS abuse is not or barely sanctioned	3	17,6%
New employees receive an account on the first day	3	17,6%
Regular check on permissions	4	23,5%
Account of employee that is leaving is immediately blocked	8	47,1%
- Periodic list HR to IT department	7	41,2%
- HR department immediately informs IT department	1	5,9%
Many problems with employees that are not often present	4	23,5%
Many problems with external users and external specialists	4	23,5%
Medical specialists work in their own cooperation	7	41,2%
Medical specialists are employed for the hospital	4	23,5%
Medical specialists do not cooperate / are stubborn	3	17,6%
Employees have high trust in colleagues and visitors	6	35,3%
Young doctors are more proficient with information technology	5	29,4%
Employees have to agree to usage policy on every log-in	1	5,9%
Medical specialists react professionally to new security measures	3	17,6%
Management is soft, no sanctions	2	11,8%
Wearing the badge is often not verified	1	5,9%