Utrecht University

Master Thesis

Submitted in fulfilment of the master's programme

BUSINESS INFORMATICS

Decoding the hype: Blockchain in Healthcare

A Software Architecture for the provision of a patient summary to overcome interoperability issues.

Erik Lau

e.lau@students.uu.nl

5796385

supervised by:

Dr. Marco SPRUIT (Utrecht University)

Dr. Matthieu BRINKHUIS (Utrecht University)

Academic Year 2017/2018

June 2018

Abstract

There is hardly any human activity which has not been positively affected by digital technologies impacting the access and exchange of information. Specifically, within the healthcare sector major improvements could be achieved. Nowadays nearly all medical records are kept in an electronic healthcare record (EHR) systems improving the access to clinical data intending to streamline costs. Electronic Health Care Records (EHRs) are however largely non-portable and kept on the systems where they have been created mainly due to interoperability, security, and liability reasons. This is resulting in a lack of medical quality for the patient and an increase of healthcare costs since the information transfer among different healthcare providers, spread over different locations, is highly dependent on the patient who is not considered as data owner and may not be aware of certain treatments received.

The objective of this thesis was to investigate how interoperability challenges within the context of Electronic Health Care Record systems can be overcome considering the patient as the owner of his patient data by taking advantage of the Blockchain technology.

In this research a software architecture has been developed from the context-, functional- and informational perspective to treat the described problem. A thorough description has been provided as to which modules are needed to assure a proper data extraction, mapping, monitoring, user access management and intervention with the Blockchain.

The proposed architecture has been evaluated based on an Architecture Trade-off analysis method which revealed, that the architecture is capable of overcoming interoperability issues by using the openEHR reference model in combination with a permissioned Blockchain solution that has been designed according to the requirements provided by the ISO 18308. The trade-off analysis revealed most strengths within the area of communication impacting the performance and medico-legal quality attributes. Furthermore, the study revealed, that Security & Privacy comes with the price of impacting the performance and the other way around.

In conclusion, it is possible to overcome interoperability issues by using the Blockchain technology for a variety of use-cases, such as the provision of a patient summary, as described within this thesis. Challenges, such as proper authorisation procedures and a mechanism to create community incentivises to maintain decentralised networks need to be further elaborated.

Keywords: Blockchain, permissioned, permission-less, EHR, openEHR, ISO 18308, Trade-Off analysis, systematic literature review, software architecture

Acknowledgement

This thesis represents the final piece for the graduation within the business informatics master program at the University of Utrecht. Many different people supported me during the research execution throughout the last nine months.

I would like to express my gratitude to my supervisor Marco Spruit for giving me the freedom and trust for conducting this research within such a novel area of technology and by always providing me with substantial feedback during the research execution. Furthermore, I would like to thank my second supervisor Matthieu Brinkhuis for his input on my thesis.

Next, I would like to elucidate my appreciation to the workshop participants willing to spend time and effort to support the validation process of the developed software architecture. Your input was highly valuable and appreciated.

Last but not least, I would to thank my family and friends for their continuous support and input during discussions in reference to the described interoperability problem impacting healthcare related matters in real-world scenarios.

Given the fact, that our society is facing massive demographic challenges within the sector of healthcare, I believe that this thesis sheds some light into the dark to aid interoperability problems by taking advantage of novel technologies to improve current deficiencies.

Table of content

Table of Figures

Table of Tables

1 Introduction

1.1 Research Background

There is hardly a human activity that has not been positively affected by digital technologies affecting the access and exchange of information. Specifically, within the healthcare sector, major improvements could be achieved. In 2008, less than 10% of medical records globally were stored electronically. This has vastly changed within the past 10 years: nowadays nearly all medical records are kept in an electronic healthcare record (EHR) systems (Adane, Muluye, & Abebe, 2013). In the 2012 edition of the Physician Sentiment Index, 81% of the questioned physicians believe that EHR systems improve the access to clinical data and more than two-thirds stated that an EHR system enhances patient care while streamlining costs (Menachemi & Collum, 2011).

Despite this progress, one major challenge remains when it comes to EHR systems: patient data stays largely non-portable. Reasons being that healthcare data is considered as complex, in terms of its data structure and meaning, which is difficult to share without a common eco-system and data standard. This problem can be described as an interoperability[1] issue which partly evolved due to independent developments of various EHR systems next to each other (Ivan, 2016). Furthermore, healthcare providers act with caution by interpreting legal requirements such as the U.S. Health Insurance Portability and Accountability Act (HIPAA). Another argument is that healthcare providers are reluctant to pass information out of privacy concerns and the fear that other parties may obtain a competitive advantage (Peterson, Deeduvanu, Kanjamala, & Boles, 2016a). This results in a lack of healthcare quality for the patient since the information transfer among different healthcare providers, spread over different locations, is highly dependent on the patient themselves who is not considered as data owner and may not be aware of certain treatments received. Hence, the patient may receive medication and diagnoses in an inefficient manner resulting in a quality decrease and an increase of healthcare costs.

This challenge has also been recognized on regional, national, and European level. The European Commission expressed within their "*eHealth Action Plan 2012- 2020 - Innovative healthcare for the 21st century"* its commitment to remove the existing barriers to *"a fully mature and interoperable eHealth system in Europe"* (Commission, 2012). A study of national laws on electronic health records in the EU Member States conducted by the Health and Food Agency (Chafea) of the European Commission revealed major disparities between countries on the deployment of EHRs for an interoperable infrastructure, that allows different healthcare providers to access and update health data. Those disparities are leaving questions unanswered in several areas within the legal and technical perspective for EHRs (Millieu Ltd & Time.Lex, 2014).

Those challenges have been partly taken up by several software vendors providing an EHR system, assisting medical practitioners in the creation, storage and organization of medical records and the possibility to share those among various vendors to a limited extent while meeting national and international regulations. One main commonality of those EHR systems is, that they are designed based on the classical client-server architecture, having a centralised infrastructure.

[1] The Healthcare Information and Management System Society (HIMSS) defines interoperability as follows: *"interoperability is the ability of different information technology systems and software applications to communicate, exchange data, and use the information that has been exchanged"*. Three levels of interoperability are known for health information technology further described within chapter 3.

1.2 Problem Statement

A centralised infrastructure leads to several downsides when it comes to sharing medical data among different regions and systems. Even if the data structure and semantics could be agreed upon in order to overcome the described interoperability issues, further challenges arise in terms of security, data ownership, data consistency, and liability.

Securing data for a centralised infrastructure is a challenging task since potential attacks and exploits lead to a single-point-of-contact requiring trust for this individual authority. This implies that an extensive effort needs to be done in order to assure that patient information are secured in terms of privacy, assuring that only authorized parties are able to access the data (Peterson, Deeduvanu, Kanjamala, & Boles, 2016b). From the ownership perspective and in the legal sense, healthcare providers perceive patient data as their property (Commission, 2012). This creates unnecessary and costly obstacles for patients who need to move their medical records to another location. Current EHR systems are not designed to manage multi-institutional life time records. Therefore, patients leave data scattered across various organisations as life events take them away from one healthcare provider to another. As a result, patients and care givers lose easy access to past records while healthcare organisations run into the challenge of record maintenance: constantly modifying and updating the healthcare data in interaction with the patient, trying to catch-up to the illusive valid healthcare profile of the patient. This may lead to a bigger problem when it comes to liability questions not knowing how accurate the patient data actually is (Prakash, 2016). Another issue appears in respect to the scalability for centrally hosted EHR systems. Given the fact that patient data is continuously added, changed or removed to the EHR, it is difficult to predict what kind of infrastructure is able to cope with a continuously growing amount of data without impacting the actual performance and therefore usability. Hence, centrally hosted systems may have the possibility to upscale processing power on a short term but may face their limits on the long-term due to its predefined data architecture (Krawiec et al., 2016).

A technology which might be able to overcome those problems could be the Blockchain technology. This technology was first mentioned in 2008 within the white paper by Satoshi Nakamoto, in which he described the concept of a distributed cryptocurrency, better known as *"Bitcoin"*. This technology allows a purely peer-to-peer online cash transfer among participants without the burden of going through a middleman (i.e. financial institution) handling transactions and being in charge to prevent double-spending[2]. The basic principle of the Blockchain technology is based on timestamped transactions (blocks) hashed into an ongoing chain of a *"hash-based-proof-of-work"*, forming a record that cannot be changed without redoing the *"proof-of-work"*, better known as Blockchain. The Blockchain serves as proof for the sequence of events witnessed and attest that the created chain came from the largest pool of CPU power. One key characteristic of this architecture is that messages are broadcasted on a best effort basis among the participants, where nodes can leave and re-join the network at will, accepting the longest proof-of-work chain as an attest of what happened during their absence (Nakamoto, 2008). This architecture is by design inherently resistant to unauthorised modification of the data while autonomously managed. As a

[2] Double-spending is the result of successful spending digital cash more than once. Trusted central authorities, in the case of monetary transaction are banks, commonly used to check every transaction in order to avoid double-spending. This leads to the disadvantage, that the fate of the entire system depends on the trusted authority (Maldonado et al., 2011).

result, it is considered as a distributed ledger, recording transactions between two parties efficiently and in a verifiable and permanent way. This concept sparked a lot of interest by the media and across industries in order to improve current security and scalability problems. Further areas of application were revealed such as the exchange of electronic healthcare records for being able to overcome the initially described challenges. In the 2016 and 2017 editions of Gartners Hypecycle for emerging technologies (Gartner, 2016, 2017), the Blockchain technology has been placed on top of the "Peak of Inflated Expectations" (see Appendix A & B). At this stage, early publicity produced a number of success stories often accompanied by scores of failures. Within Gartners Hypecycle 2017 specifically for Blockchain technologies, Blockchains in Healthcare are placed in the first phase of the Hypecycle, called "Innovation Trigger" where a significant interest by the media is triggered without having a proven concept or product (Gartner, 2017) (see Appendix C).

Given the fact that the Blockchain technology is a rather new concept, very little research has been conducted. This highlights why scientific research is needed to conclude sufficiently on the realistic potential of the Blockchain technology within the context of EHRs and the described interoperability challenges to which this master thesis shall contribute.

The problem statement can be summarised as follows:

> Electronic Health Care Records (EHRs) are largely non-portable and kept on the systems where they have been created mainly due to interoperability, security, and liability reasons. This is resulting in a lack of medical quality for the patient and an increase of healthcare costs since the information transfer among different healthcare providers, spread over different locations, is highly dependent on the patient themselves who is not considered as data owner and may not be aware of certain treatments received.

1.3 Research Objective and Research Questions

The objective of this thesis was to investigate how the mentioned interoperability challenges within the context of Electronic Health Care Record systems can be overcome considering the patient as the owner of their patient data by taking advantage of the Blockchain technology.

Therefore, the following main research question have been proposed:

MRQ: *"How can the Blockchain technology overcome current EHR interoperability challenges?"*

The main research question is being answered by responding to the following sub-research-questions:

SRQ1: What are important stakeholder requirements for a Blockchain-based EHR architecture based on the current solutions available?

SRQ2: What are current Blockchain technologies available, suitable for a Blockchain-based EHR?

SRQ3: How does a Blockchain-based EHR architecture look like taking all functional and technical stakeholder requirements into account?

SRQ4: What is the behaviour of a developed architecture taking important features (stakeholder requirements) into account?

SRQ5: What are trade-offs of the developed and tested architecture for a realistic implementation?

1.4 Societal and Scientific Contribution

As mentioned, the Blockchain technology received much attention throughout several sectors. Don Tapscott, known as one of the leading authorities on innovation, media, and the economic and social impact of technology, claims that *"The Blockchain technology is likely to have the greatest societal impact for the next few decades above emerging technologies such as social media, artificial intelligence, and the internet of things."* (Tapscott & Tapscott, 2016). This might be true, given the decentralised and secure architecture of the Blockchain technology, having a positive impact on sharing assets. The idea of sharing assets throughout the globe without having adverse effects such as the described interoperability challenges or favouring powerful intermediates through remittance scams would be a great opportunity for prosperity within our society. Exchanging electronic healthcare records by using the Blockchain technology would therefore benefit not only patients by increasing the healthcare quality and decreasing costs but also provide an insight into how this technology can be applied in the context of protecting valuables such as money, identities, intellectual property, art, and scientific discoveries. The result of this thesis takes part by answering the question how likely the Blockchain technology can disrupt current deficiencies within our society from which every human would benefit for the following examples:

- Protecting rights through immutable records
- Creating a true sharing economy
- Enabling citizens to own, monetize, and protect their data
- Ensuring compensation for the creators of value

From the scientific point of view, this research contributes by providing an insight into what the most appropriate Blockchain architecture is and how it interacts with the identified stakeholder requirements. Previous research revealed limitations on the Bitcoin and Ethereum Blockchain, since both platforms are - at the time of this study - only able to process 3 to 20 transactions per second. As a reference, financial service provider such as VISA are on average capable of handling 2000 transactions per second (Xu et al., 2016). For a realistic use of the proposed solution, scalability is critical and therefore also beneficial for other use-cases. The developed and tested architecture contributes to answer those questions and enables future research within this new field of technology.

2 Research Method

As explained in the introduction, extensive research was required to answer the initially posed research question in a scientifically sound manner. This chapter elaborates on the introduction and provides an insight how the research was conducted. Therefore, the next section describes the research concept applied throughout the thesis followed by an explanation of the research approach indicating the methods used to answer the defined sub-research questions.

2.1 Design Science Concept

One of the most commonly-known research concepts for understanding and addressing problems within the area of information systems is known as design science (March & Smith, 1995). This concept is well known among researchers and has been continuously applied within the field of information systems (IS) due to its interplay among business strategy, IT strategy, organisational infrastructure, and IS infrastructure to which IS research shall contribute. Hevner et al. (2004) describes the main purpose of this concept by gaining knowledge of a problem domain by building and applying an (IT) artefact. IT artefacts are in the context of design science known as *"constructs (vocabulary and symbols), models (abstractions and representations), methods (algorithms and practices), and instantiations (implemented and prototype systems)"* (Nunamaker, Chen, & Purdin, 1990). Artefacts are therefore built and evaluated based on identified requirements to address the initially described problem. Building and evaluating artefacts is the core activity within design science concept and considered as complex since those artefacts are created in new evolving domains for which existing theories are often insufficient (Markus, Majchrzak, & Gasser, 2002). In order to assist the researcher by the creation of sufficient artefacts, the research framework described by Hevner, March, Park, & Ram (2004), provides a clear and consistent description. The IS research framework focuses on three inherent research cycles represented in Figure 1. The relevance cycle on the left represents the environmental context initiating the design science research from which all necessary research requirements shall be derived as input for the design cycle. In return, the relevance cycle indicates if all criteria of the developed artefact are met and if additional iterations are required for further development. The rigor cycle on the right provides the base of existing knowledge within the research field in order to assure an innovative contribution of the developed artefact. Those two cycles are crucial for the design cycle since they provide the necessary background and requirements for the desired artefact development. The design cycle itself describes the iteration between the artefact development and evaluation to further refine the design of the artefact based on the rigor and relevance cycle (Hevner, 2007).

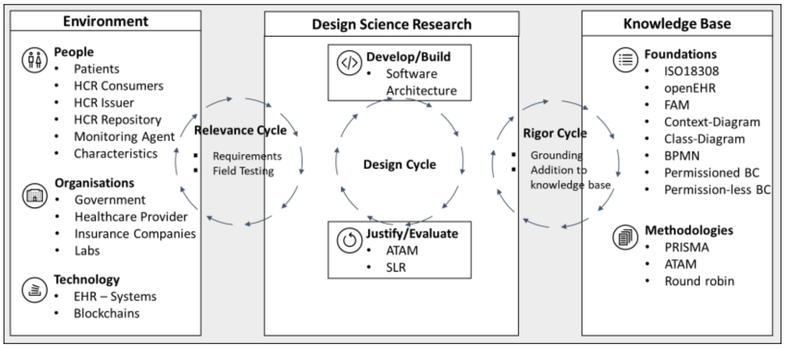


Figure 1: IS Research Framework (own creation in reference to Hevner et al., 2004)

In order to apply this framework accordingly and to understand the requirements properly, Hevner provides a seven-step guideline to assist the researcher in executing design science in an effective and complete manner. These guidelines are indicated in Table 1 and adapted to the context of this thesis.

Design Science Guideline			
#	**Guideline**	**Description provided by Hevner**	**Adapted description**
1	Design as an Artefact	Design-science research must produce a viable artefact in the form of a construct, a model, a method, or an instantiation.	Artefact 1: The Blockchain technologies categorised according to their characteristics. (SRQ2) Artefact 2: informational & functional EHR Blockchain architecture
2	Problem Relevance	The objective of design-science research is to develop technology-based solutions to important and relevant business problems.	The developed Blockchain architectures contributes in solving current EHR interoperability issues. The problem relevance was investigated by taking the relevance and rigor cycle into account.
3	Design Evaluation	The utility, quality, and efficacy of a design artefact must be rigorously demonstrated via well-executed evaluation methods.	The evaluation of the developed architectures was evaluated based on a trade-off analysis taking identified requirements into account.
4	Research Contribution	Effective design-science research must provide clear and verifiable contributions in the areas of the design artefact, design foundations, and/or design methodologies.	The research contribution is assured based on a trade-off analysis. This enhances the understanding how the designed architectures can be implemented and possibly overcome the described interoperability issues.
5	Research Rigor	Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artefact.	The research rigor was based on existing EHR systems, Blockchain technologies, health care data standards and identified stakeholder requirements.
6	Design as a Search Process	The search for an effective artefact requires utilizing available means to reach desired ends while satisfying laws in the problem environment.	The artefacts were constantly tested and adapted based on supervisor & stakeholder feedback, identified observations and test results.
7	Communication of Research	Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences.	The research was communicated through the written master thesis and the MBI colloquiums.

Table 1: Adapted Design Science Research Guidelines

Given this guideline, the design science concept has been further refined by Wieringa (2014). Within this refinement of design science, the concept is divided into the three main areas:

- *Problem investigation,*
- *Treatment Design,* and
- *Treatment Validation* entailing each guideline mentioned above.

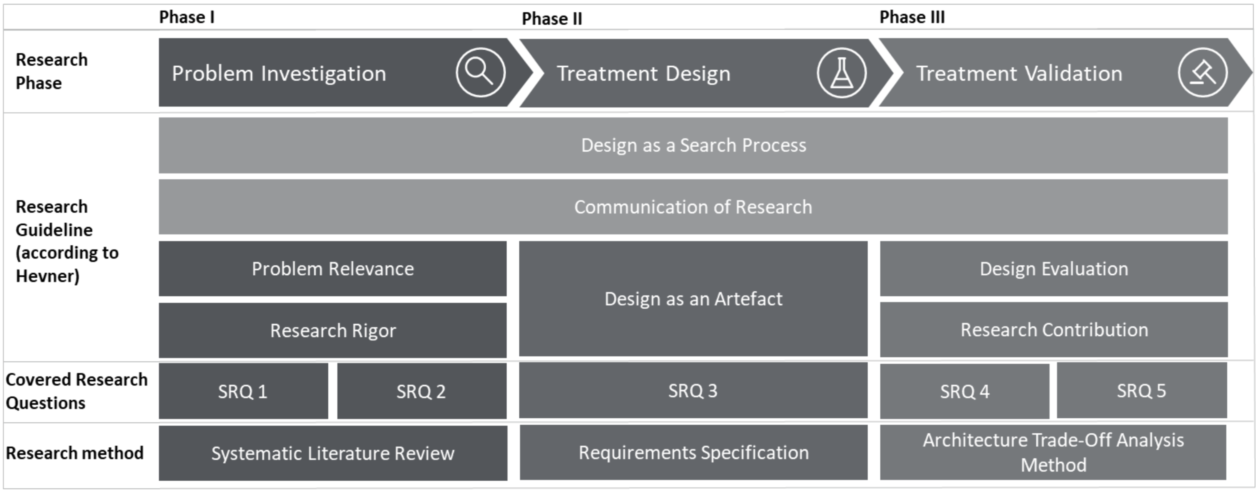
A treatment is in this case considered as an interaction between the developed artefact and the described problem, intended to treat the described problem (Wieringa, 2014). The structure introduced by Wieringa allows the researcher to focus on one area at the time of the project, assuring the introduced design science framework by Hevner (Figure1) is covered in an integrated manner. The research approach of this thesis is therefore structured according to the design science cycle of Wieringa.

A number of research methods have been introduced for the artefact design and evaluation process which are further described and mapped to the context of this thesis in the following section.

2.2 Research Approach

As mentioned within the previous section, the design science framework of Hevner adapted by Wieringa was applied. Figure 2 visualises how the research approach is structured and which parts of Hevners approach were incorporated within the design science cycle from Wieringa.

The problem investigation was the starting point of this research project preparing the treatment design by gaining knowledge about potential stakeholders, available technologies, data standards, and possible regulations. The goal of the problem investigation was to provide an answer to the sub-research question one and two. The results of the problem investigation were used as an input for the treatment design phase. Within this phase specific requirements for the artefact design of the EHR Blockchain architecture were identified and supported the designing process. As a result, sub-research question three could be answered. In the last phase, the designed treatment was validated in order to determine the effects, trade-offs, and requirements satisfied by the artefact. The goal of this phase was to develop a theory which would allow to predict the effects of the developed artefact if it would have been applied within a real-world scenario -and therefore, treat the problem of interoperability within the context of Electronic Healthcare Records by taking advantage of the Blockchain technology. The results of this phase provided an answer to sub-research questions four and five. The main research questions could only be acknowledged by answering all sub-research questions. If this would have been not the case, additional iterations of the design science cycle were executed in order to provide satisfying results.



	Phase I	Phase II	Phase III
Research Phase	Problem Investigation	Treatment Design	Treatment Validation
Research Guideline (according to Hevner)	Design as a Search Process		
	Communication of Research		
	Problem Relevance	Design as an Artefact	Design Evaluation
	Research Rigor		Research Contribution
Covered Research Questions	SRQ 1 SRQ 2	SRQ 3	SRQ 4 SRQ 5
Research method	Systematic Literature Review	Requirements Specification	Architecture Trade-Off Analysis Method

Figure 2: Proposed Research Approach (own creation)

Systematic Literature Review

The purpose of a systematic literature review (SLR) within the phase of the problem investigation was to identify what is already known about the research topic by identifying, evaluating, and interpreting available research, relevant for the posed research questions. The goal was to summarise existing evidences concerning the Blockchain technology and EHR systems, to synthesize requirements for a Blockchain-based EHR system, and to identify advantages and disadvantages of the Blockchain technology accordingly within the current technology landscape. One main requirement for performing a SLR was to execute the review in a manner that is fair and seen to be fair by applying a predefined search strategy. This provides an understanding of the research topic in a complete manner and makes it less likely that the results of the literature review are biased (Budgen & Brereton, 2006). Within this thesis the snowballing procedure was used to identify adequate evidences for the SLR by following the references from or to one paper to identify relevant papers. Snowballing can be performed both forward and backward. Backward snowballing is known by identifying related literature by following the reference list and forward snowballing is considered as an approach by identifying papers that cite the paper that has been identified as relevant (Wohlin et al., 2012). Table 2 represents which (digital) libraries were used to identify relevant literature for the SLR. Querying multiple databases assures completeness throughout the review. Identified duplicates and irrelevant literature were removed based on an initial screening of the title, author, abstract, and release year. Afterwards, all papers were screened for relevance and eligibility to further sift out relevant literature, which was in accordance to the PRISMA approach (Liberati et al., 2009). As a starting point, the search terms mentioned in Table 2 were used to identify primary literature. Limitations in terms of publicity year were applied from 2010 – 2017 to assure that only up-to-date literature was used as well for the publication language of English and German since those were known to the researcher. No limitation for the literature type were made since searching journals, conference proceedings and grey literature such as technical reports were valuable for the SLR, since the Blockchain technology is considered as rather new field without much established literature.

Keywords	**S-RQ1:** What are important stakeholder requirements for a blockchain based EHR architecture based on the current solutions available?	{electronic healthcare record*, electronic medical record*, EHR, PHR} + {architecture, system, design) + {regulations, compliance, requirements, data standard*, data sharing, interoperability}
	S-RQ2: What are current Blockchain technologies available, suitable for a Blockchain based EHR?	{Blockchain, Decentralized systems, Interorganisational system} + {electronic health care record*, electronic medical record*, EHR, PHR, EMR }

#	Search engine	Information	URL
1	PubMed	Search engine accessing MEDLINE database for life science and biomedical topics.	https://www.ncbi.nlm.nih.gov/pubmed/
2	Google Scholar	Web search engine indexing scholarly literature.	https://scholar.google.nl/
3	ACM digital library	Full text collection of all articles published by the association for computing machinery (ACM).	http://dl.acm.org/
4	Wiley Online Library	Bibliography for life, health, physical and social science articles.	http://onlinelibrary.wiley.com/
5	UCL Centre for Blockchain Technologies	University College London providing a cross-sectoral platform for the adoption and integration of the Blockchain technology offering access to all its publications.	http://blockchain.cs.ucl.ac.uk/research-papers/

Table 2: SLR Requirements

Requirements Specification

The goal of the treatment design was to provide an answer to sub-research question three. Crucial at this stage was, that the stakeholder concerns were clearly described for being able to balance conflicting priorities and to design an architecture, that addresses all requirements in an effective manner. It was important to consider that an architecture can be designed from several perspectives highlighting different viewpoints, depending on the stakeholder group. According to Rozanski (2011) several viewpoints of an architectural design exist. Due to the novelty of the Blockchain technology, the following two viewpoints were considered within the treatment design:

Functional Viewpoint:

This viewpoint describes the functional elements of a Blockchain based EHR system, taking their responsibilities, interfaces, and primary interactions into account. This view is considered as a cornerstone of most architectural views and therefore the first part of an architectural description. Furthermore, other viewpoints such as the information structure or development structure can be derived from this architecture. Other features such as the ability to change, to secure and the runtime performance of a system are significantly impacted by design decisions of the functional viewpoint motivating why such an architecture was important to design in the first instance.

Information Viewpoint:

The information viewpoint describes how the system stores, manipulates, manages, and distributes data from a complete but high-level perspective taking into account static data structures and the information flow. This viewpoint was therefore beneficial in order to provide an answer to the questions of content, structure, ownership, latency, references, and data migration which have not been explored in detail for the Blockchain technology within the context of an EHR system (Woods & Rozanski, 2012).

The goal of the treatment design was to represent both architectures in an appropriate and efficient manner without overwhelming the audience and by making assumptions which are not valid.

Rozanski (2011) describes the process for the architecture definition by following seven activities in an iterative manner which was applied accordingly during the treatment design. This was necessary in order to create a sufficient architecture for anything complex or unfamiliar such as our proposed treatment. Additionally, this approach supplements the design science methodology. The steps followed are described in a UML activity diagram within appendix D.

Architectural Trade-Off Analysis Method

The goal of the treatment validation phase was to describe how the developed artefact interacts with its identified context and to justify if it would contribute to the identified stakeholder requirements. The treatment validation was therefore considered as an experimental process, executed in an environment where the artefact was exposed to various scenarios to observe how it responds. Within the context of this thesis, the treatment was validated through a single-case-mechanism experiment within the form of an architectural trade-off analysis method (ATAM). The objective of an ATAM is to understand the software architectures fitness in reference to multiple competing quality attributes such as security, performance and modifiability with respect to scenarios the software is likely to encounter (Barbacci et al., 1998). This validation is most beneficial when executed at an early design stage within the software development life cycle, when the cost of changing the architecture is considered as minimal. The ATAM has been developed by the Software Engineering Institute at the Carnegie Mellon University and works in general as follows: once the functional and non-functional requirements of a system have been identified and an initial architecture is proposed, each quality attribute also considered as non-functional requirement is evaluated in turn, and in isolation with respect to the proposed architecture. After the evaluation, trade-off points are identified affecting multiple attributes. Based on stakeholder opinions obtained during a workshop, the model can be refined and re-evaluated to reflect the observed feedback (Woods & Rozanski, 2012). The ATAM is executed within 9 steps comprised in 4 phases as described below:

Phase 1: Presentation

- Step 1: present ATAM method to stakeholders/evaluation subjects
- Step 2: present identified requirements to stakeholders/evaluation subjects
- Step 3: present the developed architecture to stakeholders/evaluation subjects

Phase 2: Investigation & Analysis

- Step 4: identify architectural approaches without analysing those
- Step 5: generate quality attribute utility tree for specified scenarios annotated with stimuli, responses and prioritisation
- Step 6: analyse architectural approaches elicited in step 5 to identify risks, sensitivity and trade-off points

Phase 3: Testing

- Step 7: brainstorm and prioritise identified scenarios together with stakeholders/evaluation subjects
- Step 8: analyse architectural approaches by reiterating step 6 to identify & uncover additional architectural approaches, risks, sensitivity- and trade-off points.

Phase 4: Reporting

- Step 9: Present results obtained during the ATAM

By following this approach, a deep sophisticated analysis of the architectures strengths and weaknesses can be identified. Furthermore, leads this method to a more explicit understanding of trade-offs explaining the rational to stakeholders and supports the architect’s decisions making process.

3 Problem Investigation

Having defined the research topic and -method, this chapter describes the results of the systematic literature review executed during the problem investigation phase. The goal is to provide a holistic overview of what is already known about the research topic. The chapter is divided into three parts by describing the search outcome of the SLR in the first section. The second part describes relevant terms necessary to answer the first sub-research question followed by the third section outlining current Blockchain technologies identified for being able to answer the second sub-research question.

3.1 Systematic Literature Review Search Outcome

As briefly mentioned within chapter 2, the PRISMA framework has been followed in order to identify and analyse eligible material for the systematic literature review. To gather all relevant papers a search protocol was used to log every step executed throughout the search process. The search terms described within chapter 2.3 were aligned according to the search conditions of the respective search engine based on prior test queries. This was necessary to optimise the search results by adding or removing specific search conditions. The applied search query and the number of search results per engine can be found within Appendix E. Only papers which were accessible without charges through the University of Utrecht VPN and available in English or German were extracted from the databases.

Based on an initial screening for duplicates, 55 papers related to the first sub-research question and 71 papers related to the second sub-research question were considered as a base for the SLR. As a next step all papers were assessed for their actual relevance by screening their title. In some cases, it was difficult to determine the relevance of the paper only based on the title. In that case, the paper was passed at the next stage were a relevance screening through the abstract was performed. This led to a total number of 31 eligible papers for the first sub-research question and 25 papers for the second sub-research question. Within the last stage of the paper selection process, all remaining papers were fully assessed according to the PRISMA-Checklist and by creating structured summaries per paper (see Annex F for the structured summary template). This resulted in a selection of 14 papers included in this thesis as primary literature related to the first sub-research question and 17 papers related to the second sub-research question. By performing the eligible assessment, additional papers were identified through the snowballing approach. Those papers were assessed for eligibility the same way as described before. As a result, 6 additional papers for each the first and second sub-research question were identified and added to the list of primary literature.

Overall, a total amount of 20 papers identified related to the first sub-research question and 23 papers identified for the second sub-research question were considered to answer sub-research question one and two. The results are described within the next two chapters. A visualisation of the search and selection process can be found in Annex G.

3.2 EHR Stakeholder Requirements

The systematic literature review has highlighted four areas important to answer for the first sub-research question. The section below summarises the reviewed literature for the areas of identified stakeholders, existing EHR-Architectures, available standards and states the identified requirements as an overall result for the first part of the SLR.

Identified Stakeholder and Entities

In a study which set out to determine "*a system architecture to design a patient-centric monitoring system*", Mashima & Ahamad (2012) identified the following five stakeholders important to consider for the overall system architecture of an EHR-System. Those are listed within Table 3 below:

#	Stakeholder/Entities	Description
1	Patient (Owner)	The patient is considered to be the subject of the health record as well as the owner of the health record data. The patient is therefore able to manage and grant permission for access or share their health data with trusted third parties, is however not permitted for altering the health record data (Roehrs, André Da Costa, Da, & Righi, 2017).
2	Patients Monitoring Agent	The Patients Monitoring Agent is considered as an entity residing on the network being responsible for monitoring updates and the usage of health records in order to assure transparency among the patient. The activities of such a monitoring agent are access, monitoring and reporting controls.
3	Health record Repository	The Health record repository is responsible for storing the actual health records. This can be a hospital or a trusted third party i.e. software-vendor.
4	Health record issuer	The health record issuer is the stakeholder generating the patients health data which can be hospitals, labs, medical professionals and other trusted third parties. Typical activities are creating, adding and updating the health record repository. Important to consider is, that only the health record issuer is permitted to execute those activities.
5	Health record consumer	The health record consumer has the possibility to access the patients' health records i.e. hospitals, labs, EMTs[3] and insurance companies to provide medical and financial services without altering the health record data. Important to note for the architecture and the access management is, that a consumer may be the same entity as the health record issuer (i.e. hospitals). A segregation of duties for the access and authentication rights is therefore necessary to secure the healthcare record data properly.

Table 3: Identified Stakeholder/Entities

EHR-Categorisation

Within the area of healthcare information systems and communication architectures, interrelated components such as Electronic Medical Record Systems, Electronic Healthcare Records and Personal Healthcare Records are often used interchangeably. Therefore, it is important to clarify their difference and overlaps before describing actual EHR-Architectures. Furthermore, it is important to clarify the interoperability term since the exchange of information among authorised users is known is a the single most important characteristic of an EHR-System which requires interoperability from the standardisation viewpoint. Those terms are described first followed by the architectures within the next section.

[3] EMT: Emergency Medical Technicians such as ambulance.

Electronic Health Record (EHR)

According to the ISO/TR 20514 standard (Electronic health record – Definition, scope and context), an Electronic Healthcare Record is defined as a *"repository of information regarding the health status of a subject of care, in computer processable form".* Stead et al. (2005) enhanced this definition by claiming that an EHR *"refers to any information in electronic form about a person that is needed to manage and improve their health or the health of the population of which they are a part"*. To fulfil this definition, an EHR is responsible to collect information across various healthcare systems and variety of personal information sources (Stead MD, Kelly, MD, & Kolodner MD, 2005). Furthermore, an EHR is considered as a superset of an EMR and PHR.

Electronic Medical Record Systems (EMRS)

Electronic Medical Record Systems were developed during the early 1970s to better manage healthcare information and improve healthcare quality. The main activities of EMRSs are to automate clinical practices such as recording clinical notes, covering administrative tasks i.e. scheduling and billing or placing care provider orders. Electronic Medical Records (EMR) are generated as a by-product of such administrative functions and are therefore created based on the specific requirements of the EMRS (Stead MD et al., 2005).

Personal Health Record (PHR)

Personal Health Records refer to a personal electronic collection of data containing the patient's own records, therapy notes as well as electronic copies of data from the healthcare provider (Stead MD et al., 2005). The key feature of a PHR is however, that it is under the control by the patient who is also able to alter the data. According to the ISO/TR 20514, *"a PHR can have the same architecture as an EHR while still meeting the patient requirements and can be considered in at least the following four forms:*

a) a self-contained EHR, maintained and controlled by the patient/consumer;
b) the same as a) but maintained by a third party such as a web service provider;
c) a component of an EHR maintained by a health provider and controlled at least partially by the patient/consumer;
d) the same as c) but maintained and controlled completely by the patient/consumer."

Figure 3 illustrates the significant overlap of all three record systems from the functionality perspective.

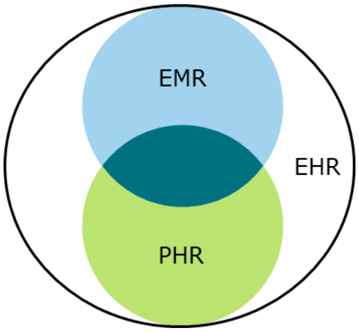


Figure 3: Interrelation EMR, PHR & EHR (own creation in reference to Stead, W., 2005)

Despite the commonalities and differences between the described record systems, healthcare data contained in those systems is used for multiple purposes by different stakeholders. The National Committee for Vital and Health Statistics defined the following three primary dimensions through which health care information can be viewed exemplified within Figure 4 (Stead MD et al., 2005):

- The patient view or Personal Health Dimension,
- The Health Care Provider Dimension (consumer/issuer),
- The community or Population Health Dimension

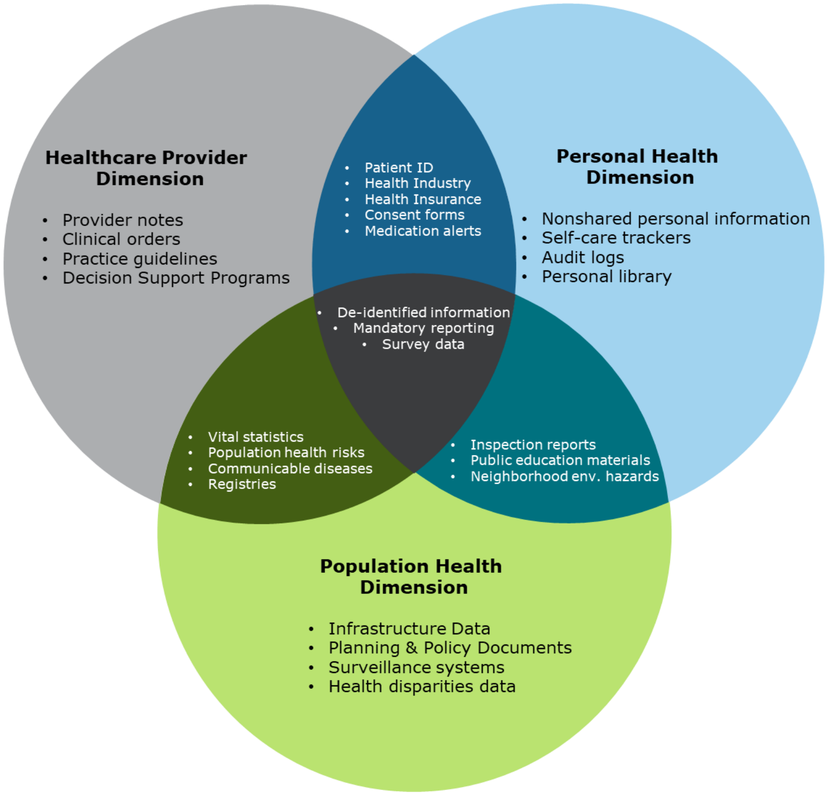


Figure 4: Health Data Dimensions (own creation in reference to Stead, W., 2005**)**

Interoperability

As briefly mentioned before, interoperability is required from the technical perspective if data shall be exchanged among different systems. According to the ISO/TR 20514 the types of functional- and semantic interoperability exist. Functional interoperability is considered as the exchange of information between two or more systems where the transmitted information is human readable by the receiver.

Semantic interoperability is known as the exchange of information between two or more systems, that is computer processable by the receiving system and no human interaction is required which is achieved through formally defined domain concepts also known as standards. The level of semantic interoperability is dependent on the level of agreement on used terminologies and templates between the systems (International Organization For Standardization, 2005).

EHR-Architecture Types

Throughout the SLR different options were noted for the classification of EHR-Architectures. Two broad categories of shareable and non-shareable EHR-Systems were identified. Non-shareable EHR-Systems can be considered as a stand-alone solution without the possibility to share EHRs beyond the immediate boundary of a single healthcare organisation. The characteristics of a shareable EHR-System is that healthcare data can be shared among different levels (i.e. between different clinical disciplines, different applications or across different EHR-Nodes). Within this thesis only shareable EHR-Architectures were considered as eligible to answer the initial research question. Although no formally defined classification exists for EHR-Architectures, the following three distinctions could be identified: centralised architecture, de-centralised architecture and semi-centralised architecture further described below (Al Jarullah & El-Masri, 2012; International Organization For Standardization, 2005).

Centralised-Architecture

The centralised architecture can be compared to the classical client-server infrastructure. Within this type of architecture, comprehensive or summarised forms of EHRs are transmitted to a central (preferably nationwide) system which is considered to be the repository for all patient records. The concept of the data transmission is known as “push-model” by which the healthcare provider is “pushing” the patient data to a central repository on a regular basis or in near-real time. Advantages of such an architecture is the system availability, performance and query response time. Known disadvantages are related to interoperability issues in terms of data context and codification. As described briefly within the introduction, other drawbacks are the increased risk of potential attacks for the central repository which requires a high level of security leading to increased design requirements and costs (Al Jarullah & El-Masri, 2012). In Europe, this approach has been adapted on a nationwide scale in Denmark, Finland, England and Estonia.

De-Centralised Architecture

The de-centralised architecture can be compared to the classical peer-to-peer infrastructure. All EHRs would be stored and maintained locally by the respective healthcare provider. A central repository would maintain references indicating the location of the patient data. This concept is known as the “pull-model” where an agent hosted on the central reference repository would request all the data which is needed from the various providers whenever a patients EHR is issued. Patient data is therefore only provided upon request leading to the advantages of data consistency by accessing the most recent version of the EHR locally. Furthermore, this architecture is known to protect patient data in a better way than central architectures related to privacy and security concerns since the patient data remains at the source instead of being duplicated at a central database. Disadvantages have been identified in terms of query performance by accessing the EHR due to unavoidable latency and incompatible security models for the data gathering process. Such an architecture is known to be appealing in theory, but the drawbacks mentioned in terms performance need to be overcome (by i.e. efficient distributed queries, short latencies and compatible security models) to have a successful de-centralised EHR (Al Jarullah & El-Masri, 2012).

In Europe, this architecture is adopted in the Netherlands known as AORTA and Austria known as ELGA.

Semi-Centralised Architecture

AlJarullah et al. (2013) presents in the paper "*A Novel System Architecture for the National Integration of Electronic Health Records: A Semi-Centralized Approach*" an architecture that benefits from both the centralised and de-centralised architecture. This architecture maintains summarised EHRs centrally and provides a reference to the comprehensive EHR stored locally at the healthcare provider. According to AlJarullah et al. is *"the idea to allow the clinicians to have an idea of what is included inside the patient's EHRs at each healthcare provider from a central location and to have a general view of the patient's medical history, and when needed, retrieve the complete EHR of the patient from a remote healthcare provider's system"*. This architecture has the advantage of fast access to summarised EHRs with the option to retrieve the full record as needed while maintaining interoperability. Despite the fact that this architecture takes advantage of both, the centralised and de-centralised approach, no countries in Europe have a national EHR following this architecture.

Table 4 represents a comparison of the described architectures per aspect derived from the SLR, mainly referring to the paper from AlJurallah et al.

#	Aspect	Centralised architecture	De-centralised architecture	Semi-centralised architecture
1	Architecture	Centralized data repository	Centralized reference links	Centralized data repository (for summarised EHR) with reference links
2	Data Redundancy	High	No	Low
3	Consistency	Low	High	High
4	Medical value	High	High	High
5	Security	Low	High	Moderate
6	Privacy	Depends on the design	High	High
7	Network traffic	Low	High	Moderate
8	Availability	High	Low	High for summaries. Moderate for comprehensive records
9	Query response	Fast	long delays due to high network traffic	Fast (for summaries)
10	Maintainability	Easy	Difficult	Difficult
11	Load balancing	Low	High	High
12	Cost/complexity of design and implementation	High	Low	Low
13	Scalability	High	Low	Moderate,
14	Mobility	High	Low	High

Table 4: EHR Architecture Comparison

Standards

Standards are used to achieve an optimum degree of order in a given context by providing rules, guidelines or characteristics for specific activities. This is achieved by establishing consensus and by an approval of a recognized body such as the International Standard Organisation better known as ISO. Within the context of EHRs, standards are useful to be applied among a variety of care settings and stakeholder to preserve the meaning of information across various application systems. The SLR revealed a wide range of different standards available and that there is currently no single universally accepted standard covering all aspects for EHR related matters (Sachdeva & Bhalla, 2012). The Healthcare Information and Management Systems Society (HIMSS) classifies Health standards into the four layers of: transport, terminology, content and security and privacy.

Transport standards address the format of message exchanges between medical systems by defining document architectures, clinical templates, user interfaces and patient data linkage. The HL7 (Health Level 7) standard is recognised as a well-known transport standard for clinical and administrative data between software applications used by various healthcare provider (Bergmann, Bott, Pretschner, & Haux, 2007; Roehrs et al., 2017; Sachdeva & Bhalla, 2012).

Terminology standards cover the requirement of effective communication between at least two systems by defining distinct communication concepts. Those concepts cover the areas of structured vocabularies, terminologies, code sets and classification systems. The main goal of terminology standards is to define the semantic of information by using consistent and computable mechanisms. Healthcare applications should therefore be able to access terminology standards in exactly the same way for being able to exchange data in a consistent manner (Tapuria, Kalra, & Kobayashi, 2013). Commonly known terminology standards would be i.e. LOINC, RxNorm or SNOMED-CT

Content standards comprise the structure and organisations of electronic messages and have overlaps with transport- and terminology standards. Content standards provide therefore definitions of common data sets for specific message types such C-CDA (D'Amore et al., 2014).

Privacy & Security standards intend to protect EHRs in terms of authorization, authentication, confidentiality, availability and integrity by providing administrative, physical and technical control mechanisms. Two types of standards are known within the context of healthcare, first standards to provide specific requirements for health information transmitted through electronic transactions such as the HIPAA and second technical security standards such as the ISO27001 standard covering Information Security Management related matters (Acharya & Kumar, 2010; Austin, Smith, & Williams, 2010).

Annex H provides an overview of healthcare data standards identified throughout the SLR grouped based on the categories described above. As it can be seen, there is a wide range of standards available, partly covering the same purpose. This makes it difficult to derive sufficient architectural requirements for an EHR-System. The ISO consolidated those requirements within the ISO 18308 standard called: *"requirements for an electronic health record architecture"*. This standard is considered to be a useful single point of reference for architectural core EHR requirements. An important feature of the standard is, that the set of requirements is provided without establishing the architecture itself. As a result, the standard can be applied in a generic way depending on the use case covering all necessary aspects of an EHR ideally suited for interoperability between heterogeneous- and legacy systems (Flores Zuniga, Win, & Susilo, 2010).

Identified Requirements

According to Gardazi et al (2017), requirements can be categorised as functional and non-functional requirements. Functional requirements specify which features are covered by a software product in this case by an EHR and are described within the system design. Non-functional requirements (also known as quality attributes) can be considered as a condition which affects the behaviour of the software which is described within the system architecture (Gardazi & Shahid, 2017). As described within the previous section, the ISO 18308 specifies the core requirements for an EHR architecture based on existing standards within the 8 points of: structure, process, communication, privacy & security, medico-legal, ethical, consumer/cultural and evolution.

The structure section covers all aspects in terms of the record and data organisation related to non-functional requirements. The section provides therefore requirements which data types are needed to a have a common data structure throughout the entire EHR.

The process section highlights all necessary requirements in order to support clinical processes such as ordering, care planning clinical guidelines etc. The goal of the requirements pointed out in this section is to support workflow processes by ensuring maximal usability and acceptability of the EHR by the identified stakeholders and the requirements are therefore considered as functional.

The communication section refers to non-functional requirements to transfer EHR data among different systems by providing requirements for messaging and record exchanges which require agreed protocols such as HL7, EDIFACT or DICOM.

The privacy & security section provides both functional and non-functional requirements to support the ethical and legal use of personal information in accordance with established privacy principles. In specific requirements for authorisation, authentication, data integrity, confidentiality, non-repudiation and auditability are provided.

The medico-legal section is mainly concerned with liability (functional) requirements to assure that every addition, amendment or alteration within the EHR is permanently recorded and preserved to assure that any evidence produced within an EHR can be trusted for all stakeholders and accepted by courts of law.

The ethical section covers all aspects in terms of the right of informed consent and the right to confidentiality with the goal to protect health. The cultural part of this section is concerned with functional requirements in order to focus on community issues involving culture and consent, expectations, languages and religious beliefs.

The last section of the ISO18308 standard is concerned with the evolution of EHR-Architectures to enable the creation and maintenance of life-time longitudinal electronic health records to ensure that the EHR system is “future proof”. The section takes both legacy requirements and new evolving technologies from the functional and non-functional requirements perspective into account.

Within Annex I a comprehensive list of ISO/TR 18308:2004 requirements can be found.

3.3 The Blockchain Technology

The SLR revealed that there is a large volume of published studies describing possible Blockchain use-cases, societal consequences and technical characteristics mainly focussing to improve Blockchain limitations on security and privacy aspects (Kewell, Adams, & Parry, 2017; Yli-Huumo, Ko, Choi, Park, & Smolander, 2016). A significant increase of yearly Blockchain related publications has been noted as of 2016 since the amount of published research papers doubled on, i.e. the ACM digital library & Wiley online library. This observation can be underpinned with the statement observed by Manski (2017) that "*US federal agencies, including the NSF, DARPA, and DHS, have awarded over $8 million to small businesses and universities for blockchain-based research*". One major weakness identified within the SLR is, that most of the studies reviewed have not been evaluated as it has been described within chapter 2. This observation has also been noted by Yli-Huumo et al., (2016) further stating that not many research papers related to other Blockchain limitations such as throughput, latency, bandwidth, versioning, hard forks, multiple chains and the issue of wasted resources exist. Overall the societal potential of the Blockchain technology has been recognized both by academia and economy. Kakavand, Kost De Sevres, & Chilton, (2017) stated therefore that: "*A review of the technical concepts of Blockchain technology is necessary to understand the implications of the different architectures with respect to performance, privacy, security and regulation.*".

The following section provides a primer to the Blockchain concepts. The first part illustrates the core components followed by the identified Blockchain types, potential hazards and downsides completed with an overview of characteristics comparing Blockchain types, describing advantages and disadvantages, mentioning identified Blockchains in order to answer the second sub-research question. Note that the Bitcoin Blockchain is used as a reference technology since it is considered as the only real proven distributed ledger from which further features, and extensions have been developed for successor technologies.

Blockchain Core Components

Several definitions of the Blockchain technology have been proposed throughout the SLR whereas no standard one exist. Linn & Koo, (2014) defines a Blockchain as follows: *"A Blockchain is a peer-to-peer (P2P) distributed ledger technology for a new generation of transactional applications that establishes transparency and trust."*. Based on this definition, three main technologies can be derived on which the Blockchain technology is based on: private key cryptography, P2P networks and network protocols. None of these technologies are new, however the orchestration and application is new.

The main purpose of private key cryptography is to create a secure digital identifiable reference to enforce a strong control of ownership. This reference is based on the possession and combination of private and public keys creating a digital signature responsible for user authentications. The intention of using a P2P network within the Blockchain context, is to reach consensus among the network members (nodes) confirming that they witnessed the same information exchange (transaction) at the same time through mathematical verification. The combination of cryptographic keys in P2P networks emerges to a useful form of digital interaction which is known to be tamper-proof. A transaction from A is made by taking its private key, announcing a transaction to the network and attach it to the public key of B. The network protocol enforces rules for the "block" creation and concatenation maintaining a history of transactions by hashing a newly created block to the previous one, which leads to the creation of the "Blockchain". The goal of the protocol is to eliminate that the same information is used in separate transactions leading to possible double spending and to assure that the blocks are considered as valid and trustworthy (Liang et al., 2017; Nakamoto, 2008; Petek, 2017). In order to reach this goal, it is important to mention, that the network size (number of nodes) is vital to aid its own security. Permission-less blockchains make use of the economic theory, which is called *"the tragedy of the commons"* to attract computing power to service the network and make it secure (Hardin, 1970). This role is served by miners offering processing power to service the network by receiving a reward for the block creation (in case of the Bitcoin Blockchain, Bitcoins). A person's self-interest is therefore used to help service the public need (Petek, 2017).

The mining process according to the *Proof-of-Work (PoW)* concept has been described by Mizrahi et al. as follows:

> 1. *"Each miner collects transactions that are broadcasted over the network and uses her hash power to try to generate a block via repeated invocation of a hash function on data that consists of the transactions that she saw fit to include, the hash of the previous block, her public key address, and a nonce.*
> 2. *When a miner succeeds in generating a block, meaning that the hash of her block data is smaller than the current difficulty target, she broadcasts her block to the network.*
> 3. *In case other miners see that this block is valid, i.e. it references the hash of the previous block and meets the current difficulty target, and see that it is the longest extension of the chain of blocks (a.k.a. Blockchain) that they are aware of, they move on to continue to extend the Blockchain from this block."* (Bentov, Lee, Mizrahi, & Rosenfeld, 2014)

In conclusion all transactions are kept in the Blockchain and are shared among all nodes. The combination of the three components mentioned earlier ensures verifiable and immutable transactions; tamper resistance, transparency, and integrity of distributed data since there is no single point of failure in the network (Zhang, 2015).

The primary interface responsible to interact with the Blockchain is a wallet proposing and accepting cryptographic records representation the value of transactions performed. The public key of a user is used in the address of a wallet to assure reachability through the network and the private key is used for the user authentication. Important to note is, that the wallet is no core component of a Blockchain system and therefore not entailing the same security characteristics (Yli-Huumo et al., 2016).

A component leading to more flexible application for Blockchains is known as a smart contract. Smart contracts are considered as an application automatically moving digital assets based on arbitrary pre-specified rules throughout the Blockchain network. This can be for example a currency withdrawal rule or a pre-defined user access right. Smart contracts are executed sequentially by the network of mutually distrusting nodes without the arbitration of a trusted authority. This concept was introduced first by the Ethereum Blockchain including the feature that smart contracts can be triggered and executed by transactions or function calls from other contracts. Many other concepts for smart contracts have been introduced, whereas each Blockchain technology has its own specification and therefore advantages and disadvantages (Bartoletti & Pompianu, 2017; Buterin, 2014; Zhang, 2015).

Blockchain Types

Generally, Blockchain technologies can be classified into the types of: permission-less, permissioned and hybrid systems.

The main characteristic of permission-less Blockchains, such as Bitcoin or Ethereum, is that the identities of nodes are either pseudonymous or anonymous having the possibility to join and leave the network at their will and provide hashing power through miners. The design of permission-less Blockchains is useful for the exchange of values where the identification of nodes is negligible as long as there is consensus. This design might not be adequate for business applications due to a number of reasons such as increased network instability risks for nodes suddenly leaving the network and hence clogging the throughput, which should be in particular avoided for healthcare data (Dubovitskaya, Xu, Ryu, Schumacher, & Wang, 2017).

Permissioned Blockchains provide similar characteristics as permission-less Blockchains, operate however in environments where the participants have verified identities and are invited to participate by accepting specific user-access rights. This can be useful for business applications having the requirement of identified nodes due to legal and compliance reasons. As a result, the mechanism to reach consensus among the distributed nodes, which is achieved for permission-less Blockchains through PoW, can be achieved based on state machine replication algorithms (Dubovitskaya et al., 2017). The SLR revealed that byzantine-fault-tolerance (BFT) algorithms are commonly used for permissioned Blockchains to reach consensus. Pease, Shostak, & Lamport, (1980) describe that at least $3f + 1$ nodes are necessary to reach consensus in the presence of up to f Byzantine faulty nodes (Gervais et al., 2016; Vukolić, 2017). Note, that BFT deployments can only scale to a limited number of nodes, hence, more network participants lead to worse performance but is in comparison to PoW faster. Furthermore, requires this concept a (logically) centralised identity management where trusted parties issue identities and cryptographic certificates which is considered as a disadvantage to permission-less environments (Luu et al., 2016). Examples for permissioned Blockchains are Ripple, Hyperledger-Fabric/Sawtooth and Tendermint.

The philosophy of hybrid systems is to take advantage of the described Blockchain characteristics without having its disadvantages or advancing on the current architecture. A general characterisation and classification of those hybrid technologies is difficult to achieve due to the variety of solutions available. An example for such a technology would by “the tangle” which is the underlying technology of IOTA and considered to be a directed acyclic graph (DAG) for storing transactions. The tangle has been developed for Internet-of-Things (IoT) applications with a high transaction throughput without requiring transaction fees. According to the white paper, every node in the network executes transactions and participates therefore in the consensus. This happens in particular by validating at least two transactions directly and other transactions in the sub-tangle indirectly. This way, validations can be performed in parallel while the network stays decentralised without having the need for PoW. This principle makes the system highly scalable, as long as enough nodes are participating (Popov, 2017). BigchainDB can be considered as another hybrid technology by following the philosophy of “blockchainifying” a big data database such as NoSQL (in case of BigchainDB, a MongoDB) with consensus algorithms (BFT) on top of the database layer. Blockchain characteristics such as decentralization, immutability and built-in support for creation & transfer of assets is assured with a relatively high scalability (avg. 1000 transactions per second) compared to common Blockchain solutions (Mcconaghy et al., 2016).

Potential Hazards and Downsides of Blockchain Technologies

Despite the earlier mentioned advantages of Blockchains, the current PoW consensus raises concerns in terms of the general network security, since a potential attacker could add so many nodes[4] that he effectively controls the mining hash rate of the network and could therefore manipulate the Blockchain validity. This malicious intent is known as Sybil attack. Up until now, the Bitcoin Blockchain has proven to be capable of resisting those attacks by making the attempt prohibitively expensive (Bentov et al., 2014; Dubovitskaya et al., 2017; Mcconaghy et al., 2016). Another malicious intent applicable for PoW Blockchains is known as selfish-mining. According to Gervais et al., (2016) is the principle that miners attempt to perform selfish mining attacks to increase their relative share of nodes similar the Sybil attack. The catch for this attack is that mined blocks are selectively restrained and only gradually published to the network. This is resulting into a longer and more difficult chain for the remaining nodes to adopt while the attacker claims the mining reward for himself[5]. Both types of attacks could result in double-spending or PoW-denial-of-service attacks refusing to include transactions in the blocks and harm the overall performance and confidence in the network. Further downsides related to PoW environments are scalability aspects (latency & throughput). As mentioned earlier, latency issues since the creation of a block takes for the Bitcoin Blockchain approximately 10 minutes whereas a confirmation of transactions should happen in (milli-) seconds, while maintaining security. Another drawback which is often ignored is the waste of resources of electricity for PoW environments since the mining process, which requires specific hardware (ASIC modules), consumes a large amount of energy. The Bitcoin Energy Consumption Index[6] estimated the Bitcoin annual electricity consumption (TWh) in December 2017 with 31.7 TWh which is comparable to the annual electricity consumption of Serbia or to 2,926,153.00 U.S. households. Other consensus mechanisms such as Proof-of-Stake (PoS) might have the potential to mitigate those disadvantages and are currently under development (Bentov et al., 2014; Luu et al., 2016; Petek, 2017; Vukolić, 2017).

Other downsides related to PoW which have been identified throughout the SLR are the following:

- Transactions are not fully anonymous
- Not scalable to global economy nor to large company requirements
- Transactions costs are unpredictable and might increase
- The ledger is only theoretical immutable (no finality)
- Mining is overly centralised (see Appendix J)

Table 5 describes identified Blockchain characteristics and compares them between permissioned and permission-less environments. Furthermore, advantages and disadvantages are pointed out followed by general Blockchains and use cases identified within the area of healthcare related records. Note that the table has been created based on the results of the SLR mainly referencing to the studies of Nakamoto (2008).

[4] This point is reached when more than 50% of the nodes are in control by the attacker

[5] According to Garvais et al. (2016) have recent studies shown, that a selfish miner equipped with originally 33% mining power can effectively earn 50% of the mining power. Annex I contains an overview of the current (December 2017) mining pool distribution.

[6] Digiconomist. (2017). Bitcoin Energy Consumption Index - Digiconomist. Digiconomist, 1–8. Retrieved from https://digiconomist.net/bitcoin-energy-consumption

Attribute	**permission-less (PoW)**	**permissioned**
Decentralised	**yes (fully)**	yes (semi)
Immutability	**yes (not finally proven yet)**	yes (depending on the flavour)
Node identity management	**open, entirely decentralised**	closed, node IDs need to be known among participants
Consensus finality	no	yes
Scalability (# of nodes)	**excellent (thousands of nodes possible)**	limited
Scalability (# of clients)	**excellent (thousands of clients possible)**	**excellent (thousands of clients possible)**
Performance (throughput)	limited	**excellent**
Performance (latency)	high-latency	**excellent**
Power consumption	very poor	**good**
Tolerated power of an adversary	< 25% computing power	< 33% voting power
Network synchrony assumptions	physical clock timestamps (enforced by protocol)	**none for consensus safety**
Correctness proofs	no	**yes**
Deployment style	public	private or public
Business context	Inter-entity across a network or ecosystem	Inter-company or across an industry
Accountability, Legal Standing	limited/zero legal accountability and unregulated actors	**legally accountable**
Consents Mechanism	- Proof-of-Work	- Proof-of-Stake - Practical Byzantine Fault Tolerance - Deposit Based - Federated Byzantine Agreement
Advantages	- All data public/transparent - Ability to resist malicious attempts - no centralised entity control - no separation of users from application developers - Ecosystem growth via. Network effect - open source - "Unlimited" developer resources - "Unlimited" native asset creation	- Authenticated and secured by known user rights - optimisation of protocols and the network for specific use cases - shared network/management utility costs - easier governance and policy enforcement - open to regulatory oversight - controlled standard development - operationally faster - underlying product/service/business model stability and protection
Disadvantages	- scalability issues created transaction latency - complicated governance - untrusted actor participation - potential for mining concentration - potential for illegality - Direct financial incentives required to maintain the network	- single point of failure - may not be fully open source - reinforces existing business models and process sets - maintains existing supplier product fee structures - limited developer resources requires corporate consensus
Classified platforms (non-exhaustive)	HAWK, Bitcoin, Counterparty, Elastico, Enigma, Ethereum, Hasq, IOTA, LaZooz, Lisk, Mastercoin, Matterium, Namecoin, Peercoin, ProvChain, Stellar, Swarm	Corda, BigchainDB, DRAMS, Microsoft Azure (Coco framework), Monax, Monero, Ripple
Classified platforms for Healthcare purposes (non-exhaustive)	N/A	- Hyperledger (with various frameworks i.e. Fabric/Sawtooth) - Patientory - MedShare - MedRec

Table 5: Blockchain Type Comparison

4 Architecture Design & Characteristics

Having performed the problem investigation covering sub-research question one and two, this chapter focusses on the treatment design by specifying the identified requirements necessary to design an appropriate functional and informational architecture for being able to answer sub-research question three. As discussed within chapter 2, the architectural definition activities were followed according to Rozanski (2012) (see Appendix D).

4.1 Architecture Design

To produce a solid baseline, all non-functional stakeholder concerns identified throughout the SLR were consolidated as a first step and are represented within the table below.

#	Non-functional requirement	Description
1	Security & Privacy	The architecture must provide appropriate measures in terms of user authorisation, authentication and the possibility to audit/monitor actions performed with the ability to detect and recover from security failures.
2	Performance	The architecture has to offer the ability to execute predicted performance measures with the possibility to handle increased processing volumes (transaction throughput).
3	Communication	The architecture has to offer the ability to exchange patient data among a various number of systems in a semantic interoperable manner.
4	Medico-Legal	The architecture has to offer the ability to stay complaint with national and international regulations covering liability aspects.
5	Evolution	The architecture has to offer the ability to be flexible regarding to inevitable changes after deployment.

Table 6: Non-Functional Requirements

As a second step of the architectural definition process, a scenario likely to be encountered by the architecture was selected. This activity is important in order to illustrate relevant requirements of the system allowing an assessment of the effectiveness of the architecture in that specific situation. As mentioned before, interoperability is considered as a complex issue which needs a structured and cohesive approach in order to be tackled. The eHealth Stakeholder report on perspectives and recommendations for interoperability identified nine priority scenarios which have been widely adopted and mature specifications exist (see appendix K). The number one scenario according to the report is the provision of a patient summary on national and cross-border level (eHealth Stakeholder Group, 2014) which has been selected as a use-case for this thesis. The selected use-case scenario tackles the following activities by taking the mentioned non-functional requirement into account (see table 7). Please note that table 7 is a high-level description of the use-case scenarios, a detailed use-case description can be found in Appendix L, describing the use-cases, required applications, preconditions, triggers, basic- and alternative flows for the scenarios.

Use-Case Scenario: provision of a patient summary on national and cross-border level		
ID	**Use Case Name**	**Use Case Description**
U1	Provision of a single patient summary	Obtain patient summary from a remote system for the first time/since the last change.
U2	Provision of multiple patient summaries	Obtain multiple patient summaries from remote system for the first time/since last change in one batch.
U3	Provision of previous patient summary versions and revision histories	Obtain version and revision history of a patient summary from a remote system.
U4	Systematic update requests	1. Periodic update of changes to the patient summary since last change for a specified period. 2. Event driven update due to certain event on the patient summary occurred.
U5	Access Monitoring	Provide access monitoring information according the patient summary access permissions.

Table 7: Functional Requirements - Patient Summary

Having defined the functional requirements, use-case diagrams per scenario have been designed (see Appendix M). Figure 5 represents all scenarios summarised in one use-case diagram by expressing the relationships between the use-cases (functional requirements), actors (stakeholders) and the proposed system (EHR Patient Summary System). Note that the diagram does not represent the order nor technical description in which the activities are performed to achieve its goal, rather the kind of activities covered in relation to its actors. This is beneficial to provide a graphical and simplified overview of what the system shall do as a first design step.

As it can be seen within the Use-Case diagram in figure 5, each stakeholder is at least involved in two use-cases. The Patients Monitoring Agent is responsible for monitoring the patient summary version & revision history as well as the user access to the patient summary. The user access rights are defined by the patient who can access his patient summary including a version and revision history and access reports of users eligible and attempting to access their patient summary. The Healthcare Record issuer has also the possibility to consult the patient summary version and revision history and is eligible to perform changes (add, change or delete data) within the patient summary which is represented in the "Update request" use-case. The Healthcare Record Consumer can consult the patient summary version & revision history and is eligible to access single and multiple patient summaries depending on the defined user access rights. The Healthcare Record Repository is responsible for providing the data for the patient summary according to the cross-border directive 2011/24/EU Release 1 (providing minimal requirements of a patient summary) by obtaining the patient data from the legacy EHR systems, converting the data to a commonly accepted data standard and eventually providing the patient summary data to all stakeholders involved. Note that lines represented in the use-case diagram are considered as associations between the actors and use-cases. Lines with arrows represent generalisations of use-cases by indicating that this use-case is covered by the activity the arrow is pointing at.

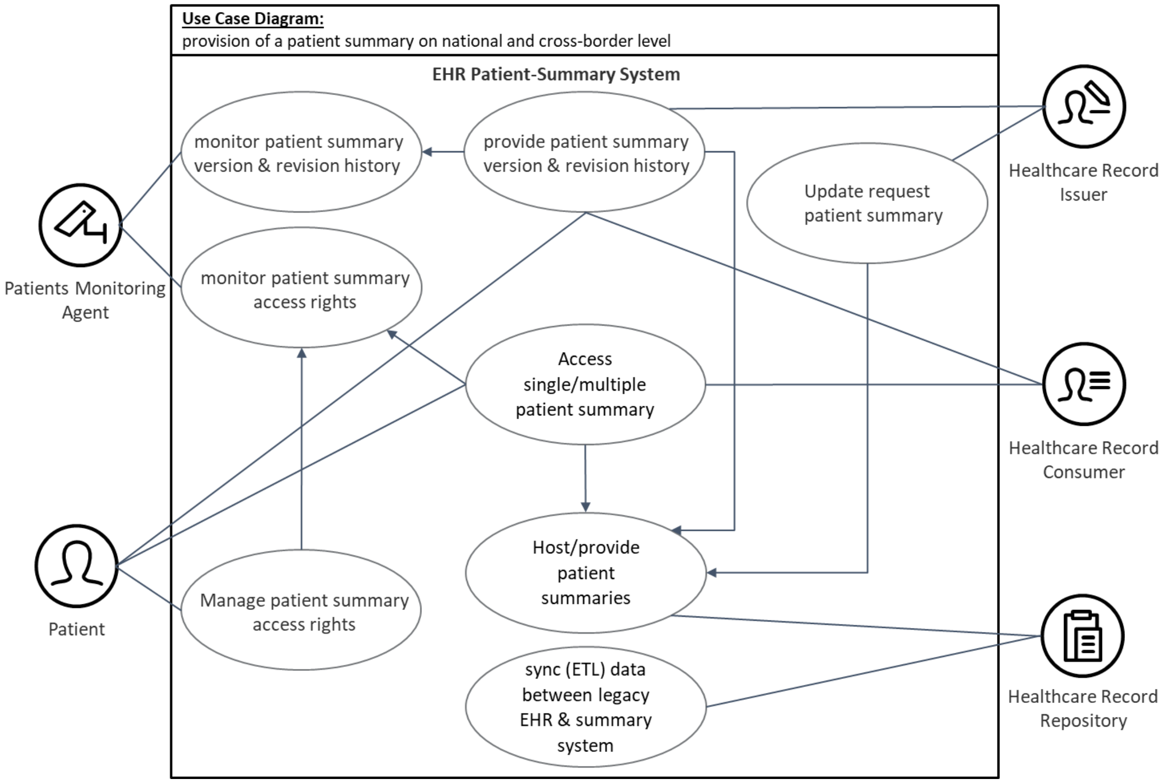

Use Case Diagram:
provision of a patient summary on national and cross-border level
EHR Patient-Summary System
monitor patient summary version & revision history
provide patient summary version & revision history
Update request patient summary
Healthcare Record Issuer
Patients Monitoring Agent
monitor patient summary access rights
Access single/multiple patient summary
Healthcare Record Consumer
Host/provide patient summaries
Patient
Manage patient summary access rights
sync (ETL) data between legacy EHR & summary system
Healthcare Record Repository

Figure 5: Use-Case Diagram - Patient Summary System

4.2 openEHR

For being able to design a future proven architecture in line with standards available, the openEHR framework is known to provide guidelines ideally suited to build comprehensive EHR-Systems technically validated by domain experts and compliant with the most common data standards and regulations such as HL7, SNOMED, C-CDA and ISO 13606 (Sachdeva & Bhalla, 2012). The openEHR foundation is an independent, open and a non-profit organisation founded in 2000 by the University College London and Ocean Informatics with the goal to enable the development of portable, vendor-neutral software specification for EHR Systems (Kalra, 2006; Lin, Fann, & Liou, 2016; Teodoro, Sundvall, João Junior, Ruch, & Miranda Freire, 2018). The solutions provided span from requirements, abstract specifications, implementation technology specifications (ITS), computable expressions and notations for conformance criteria focusing on systems and tools necessary for the computation of complex and constantly evolving health information at the semantic level. The paradigm used by openEHR is a two-level modelling approach by separating the semantics of information and knowledge into small reference models (RM) used to build information and knowledge models and Archetypes[7] in order to apply domain concepts by following formalised structures (see figure 6). The goal of the RM is to represent general health record features, organisational methods and necessary contextual information by providing a set of general reusable building blocks. RM support therefore medico-legal requirements and record management functions in order to ensure an interoperable information transfer. Archetypes are used to define entire and coherent informational concepts for clinical domains and can be re-used depending on the use-case. Existing archetypes can be re-defined or extended through sub-classing. OpenEHR templates enable to combine several archetypes and modify those according to the required specification (Kashfi & Torgersson, 2009). By applying this approach, it is possible to design EHR-Systems on a stable reference model as a general framework and by using archetypes as domain information model to achieve a greater level of flexibility and stability under continuously evolving requirements (Santos, Bax, & Kalra, 2010; Tapuria et al., 2013; Wang, Min, Wang, Lu, & Duan, 2015). The openEHR framework has therefore been used for the design of the software architecture since the framework focuses on semantic interoperability in order to improve the quality of data exchange among a variety of organisations and systems.

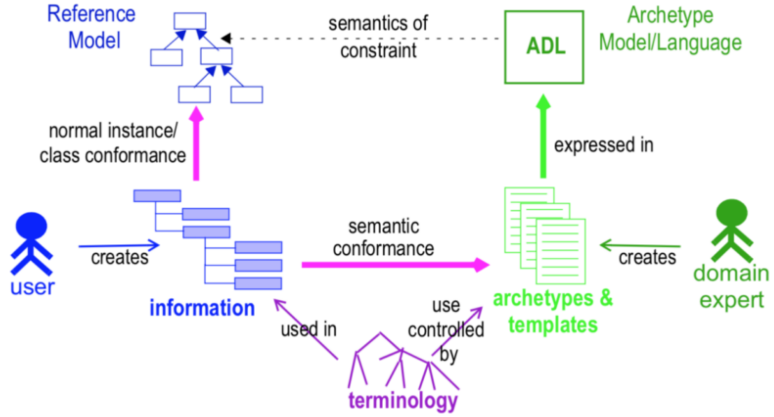


Figure 6: Archetype Meta Architecture [Baele & Heard, 2007]

[7] An archetype is a hierarchical combination of components from the RM with available restrictions placed on names, possible data types, default values, cardinality, etc. These structures, although sufficiently stable, may be modified or replaced by others as clinical practice progresses and evolves [43]

4.3 Functional Architecture

According to Brinkkemper & Pachidi (2010), several recommendations have been provided to develop an elegant functional architecture which has similarities to the approach described by Woods & Rozanski (2012). After the definition of the functional and non-functional requirements as well as by selecting architectural styles, a skeleton architecture has been developed according to the Functional Architecture Model (FAM) described by Brinkkemper & Pachidi (2010) representing the main functions of the proposed architecture which can also be considered as candidate architecture (see figure 7). This approach has the advantage that the skeletal system can be used for incremental growth and expansion of the architecture which is in line with the described design science approach by Hevner et al. (2004) assuring that the treatment undergoes several design iterations.

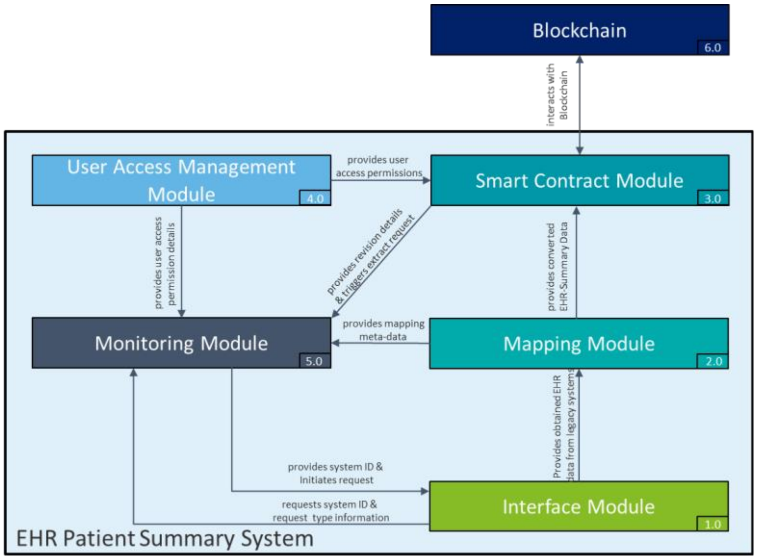

Blockchain
6.0
interacts with Blockchain
User Access Management Module
4.0
provides user access permissions
Smart Contract Module
3.0
provides user access permission details
provides revision details & triggers extract request
provides converted EHR-Summary Data
Monitoring Module
5.0
provides mapping meta-data
Mapping Module
2.0
Provides obtained EHR data from legacy systems
provides system ID & Initiates request
requests system ID & request type information
Interface Module
1.0
EHR Patient Summary System

Figure 7: High-Level Functional Architecture

Figure 6 represents the primary functionality of the patient summary system for all stakeholders involved. Within Table 8, the functionalities have been described per module displayed.

Element ID	Element Name	Element Description
1.0	Interface Module	- retrieve patient summary data from various EHR-Systems independent of the clinical standard according to cross-border directive 2011/24/EU Release 1 - manage all interface sessions to legacy systems - assures that interface connections are properly secured - assures proper data traffic to legacy systems without impacting operational activities
2.0	Mapping Module	- convert obtained patient data to openEHR data standard - assures completeness & integrity - creation of patient summary
3.0	Smart Contract Module	- triggers extract request for patient summary - issue patient consent - verify, upload and monitor the patient summary to the Blockchain
4.0	User Access Management Module	- manage user-access rights to the patient summary which are transferred and executed by the Smart Contract Module
5.0	Monitoring Module	- responsible for logging and monitoring user accesses and changes related to the patient summary performed
6.0	Blockchain Module	- hosts the patient summary on the Blockchain

Table 8: Description of Module Elements

Functional View: Interface Module

Retrieving data from a variety of legacy systems is one of the most basic requirements to be satisfied by the proposed architecture. Typical data sources include i.e. relational databases, HL7 messages, CDA documents and other data sets which need to be converted on syntactical and semantical level. The goal of the interface module is to retrieve patient data from multiple sources and to provide the data for the conversion to a standardized (openEHR compliant) patient summary. See figure 8 for the functional architecture of the Interface Module according to the FAM.

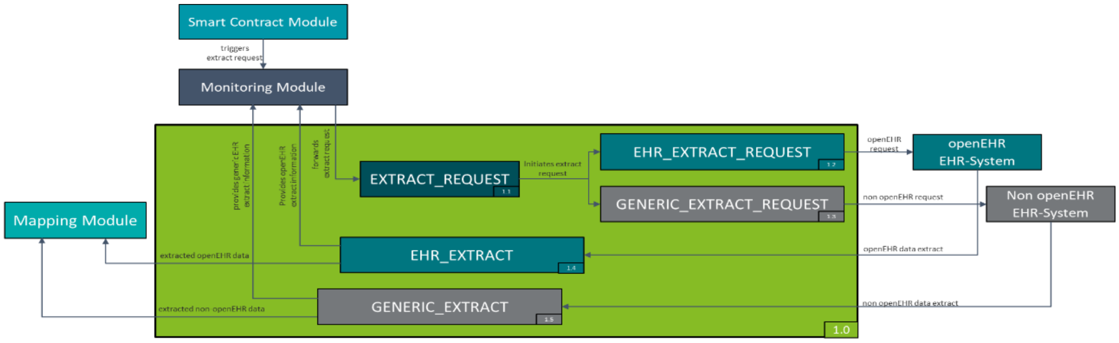


Figure 8: Functional View - Interface Module

The process for retrieving the patient data starts based on the proposed interface module with an extract request for "information from the record of one or more 'subjects'" triggered by the Smart Contract Module and forwarded through the Monitoring Module providing information of potentially previous performed requests. Note that at this point the request shall not be intelligent in any way, instead identify the appropriate system through the monitoring module and extract the content available.

A patient record is considered as a record in a demographic system or any other logically meaningful top-level entity. A distinction of requests is made for systems which run under the openEHR reference model or any other data standard/reference model. The requests contain a detailed specification of the content to be obtained for a defined time period and security requirements under which the data shall be extracted. The security requirements are important for the potential risk of exposure since the responding systems are supposed to be in an uncontrolled environment outside the described system boundaries and hence applied security policy. Table 9 below summaries and describes the indicated elements of Figure 8.

Element ID	Element Name	Element Description
1.1	EXTRACT_REQUEST	- triggers the extract request for one or more patients upon event or defined period (batch) - specifies time period of extract FULL/UPDATE - FULL: request is made for all available data - UPDATE: request is made since the last request executed
1.2	EHR_EXTRACT_REQUEST	- provides request semantics for openEHR related systems
1.3	GENERIC_EXTRACT_REQUEST	- provides request semantics for non-openEHR related systems
1.4	EHR_EXTRACT	- provides extracted data according to openEHR syntactic & semantics
1.5	GENERIC_EXTRACT	- provides extracted data according to non-openEHR syntactics & semantics
5.0	Monitoring Module	- provides demographic information of the feeder system - provides information of requests performed in the past - receives and updates repository based on requests performed
3.0	Smart Contract Module	- triggers patient summary request

Table 9: Description - Interface Module

Functional View – Mapping Module

The purpose of the mapping module is to convert the patient data, retrieved from various EHR systems, into a form compliant with the openEHR reference model in order to create a patient summary. As mentioned before, the patient summary contains *"the minimum set of information needed to assure healthcare coordination and the continuity of care"* according to the guidelines provided within the cross-border directive 2011/24/EU by the European Commission (eHealth Network, 2013). The patient summary dataset can be found within Appendix N and the functional view of the mapping module to create the patient summary is described within figure 9.

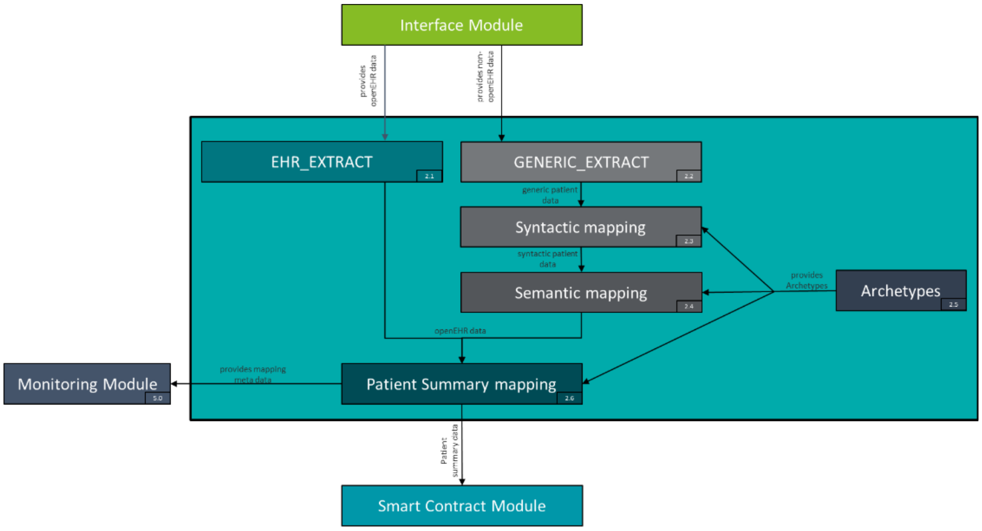


Figure 9: Functional View - Mapping Module

As it can be seen, the data retrieved from the source systems is provided by the interface module. A conversion is only required when the data is provided as a generic extract, performed in two steps. Within the first step, a syntactic mapping is executed by converting the source data from its original form to a format obeying the openEHR reference model. The data converted is controlled by rules deployed through an archetype designed to mimic the incoming data structure (such as HL7) and to create versioned compositions of the extracted data. In the second step, a semantic transformation is performed in order to convert the data to a standardised clinical archetype where the terminology is in common. Furthermore, meta-data is added during the conversion process to add medico-legal audit information of the originating system and conversion details. Once the data is in line with the openEHR framework the patient summary is created by mapping the obtained data to the desired patient summary dataset. The meta data created on the patient summary is also provided to the monitoring module for medico-legal reasons. The rules for the semantic and patient summary mapping are provided by pre-defined archetypes.

Element ID	Element Name	Element Description
2.1	EHR_EXTRACT	- provides extracted data according to openEHR syntactic & semantics
2.2	GENERIC_EXTRACT	- provides extracted data according to non-openEHR syntactics & semantics
2.3	Syntactic mapping	- performs openEHR syntactic data mapping
2.4	Semantic mapping	- performs openEHR semantic data mapping
2.5	Archetypes	- entails rules for the archetypes in order to perform syntactic, semantic and patient summary mapping
2.6	Patient Summary mapping	- performs patient summary mapping - provides mapping meta-data to monitoring module

Table 10: Description - Mapping Module

Functional View – User Access Management Module

The purpose of the User Access Management Module is to meet the Security and Privacy requirements. The EHR must therefore offer the ability to define, attach, modify or remove access rights for classes of users and offer the possibility to control the access rights of all users involved (International Organization for Standardization, 2005). According to the openEHR reference model, there is currently no formal proven model available, managing user access rights for shared health information. Thus, the openEHR framework provides only a simplistic and flexible access control model which need to be tailored depending on the application. According to Ferraiolo, Kuhn, & Chandramouli (2003) role based access control (RBAC) systems support policy neutral role hierarchies and constraints where a wide range of security policies can be expressed. Other advantages of RBAC systems are that the security administration is greatly simplified by the use for roles to organise privileges and the possibility to reduce the risk of fraud due to segregation of duty violations. Figure 10 represents the functional view of the RBAC based user access management module designed for the proposed EHR patient summary system.

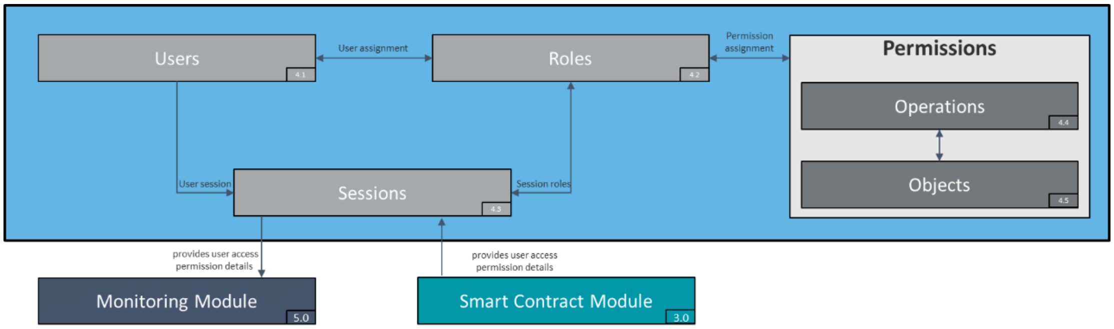


Figure 10: Functional View - User Access Management Module

The basic concept of the represented module is that users are assigned to specified roles defined by operation- and object permissions. Users acquire therefore permissions by being members of those roles. The resulting relationship between user-roles and permission-roles can be many to many. Furthermore, the module includes the concept of user session, allowing a selective activation/deactivation of roles depending on the desired operation. This is in particular useful to assure a segregation of duty between the Healthcare Record Issuer and Health Record Consumer, which could be in the case of a doctor one and the same person (as described within chapter 3) with the premise, that only the doctor under the role of the healthcare record issuer is allowed to perform changes to the healthcare summary. Table 11 summaries the functionality of the user access management module.

Element ID	Element Name	Element Description
4.1	Users	- Users represent the actors in the system being assigned to different roles depending on their functionalities
4.2	Roles	- Roles are considered as job functions entailing access permissions depending on the job purpose
4.3	Sessions	- Sessions entail the assigned roles depending on the activity of the user - User access rights are provided from the Smart Contract- and to Monitoring Module
4.4	Operations	- Operations define the type of activity performed on a defined object, this could be read, write or execute operations
4.5	Objects	- Objects are considered as an entity within the system that contains/receives information i.e. the created patient summary

Table 11: Description - Mapping Module

Functional View – Monitoring Module

The purpose of the monitoring module is to assure that all changes performed to the healthcare record are audit-trailed, all previous states of the record are available for the purpose of medico-legal investigations (in line with ISO 18308) and the record is kept in a consistent informational state according to the user access rights and conversion rules. The informational view of the designed monitoring module is represented in figure 11 below.

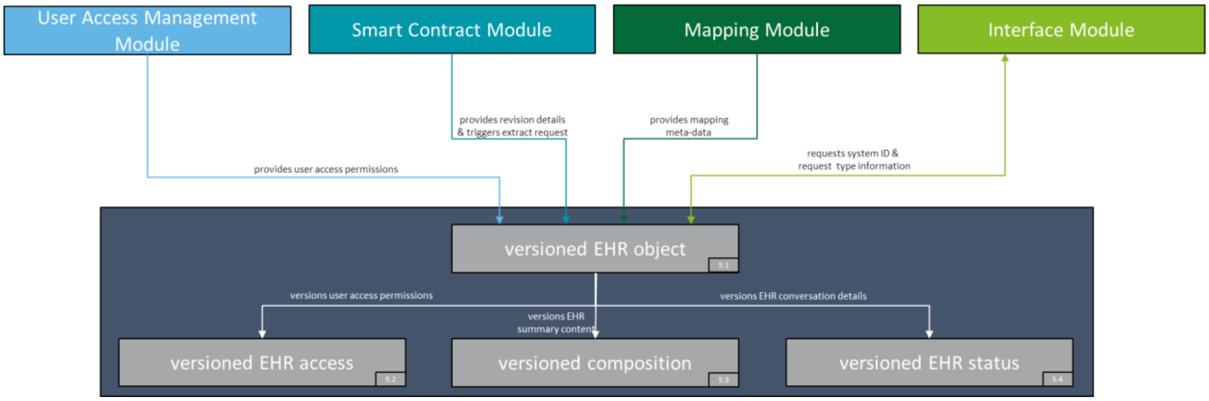

User Access Management Module
Smart Contract Module
Mapping Module
Interface Module
provides revision details & triggers extract request
provides mapping meta-data
requests system ID & request type information
provides user access permissions
versioned EHR object
5.1
versions user access permissions
versions EHR conversation details
versions EHR summary content
versioned EHR access
5.2
versioned composition
5.3
versioned EHR status
5.4

Figure 11: Functional View - Monitoring Module

As it can be seen the monitoring module contains four elements following the openEHR reference model. The versioned EHR object contains data about where the EHR data is originating from to allow the repository to be properly versioned. Information is distinguished to enable the detection of duplicates and new versions. The versioned EHR status element deals with a number of aspects occurring during the data conversion process. It creates meta data for the items from the originating systems to enable a proper versioning of the EHR data and to identify those accordingly. The versioned EHR access element contains all information about access rights granted over time and the versioned composition container contains all clinical and administrative content of the record created, changed or deleted mainly for medico-legal reasons. See table 12 below for a summarised description of the elements.

Element ID	Element Name	Element Description
5.1	versioned EHR object	- main element responsible for a proper versioning of EHR data regarding to the sub-elements provides data of: - subject identifier - location of the legacy system - identifier for legacy system - identifier of request - identifier of the information item used by the legacy system - timestamp(s) assigned by legacy system to the item
5.2	versioned EHR access	- containing access control settings for the record
5.3	versioned composition	- container of all clinical and administrative content of the record created, changed or deleted over time
5.4	versioned EHR status	provides meta data of the data conversion process: - system type/standard - type of request - agent who committed the item - status of information, e.g. interim, final - version id, where versioning is supported

Table 12: Description - Monitoring Module

Functional View – Smart Contract Module

The purpose of the smart contract module is to act as an interface for the created patient summary enforcing the user permissions on the Blockchain and tracking any changes performed to the patient summary. The module consists out of four elements which are represented within figure 12 below.

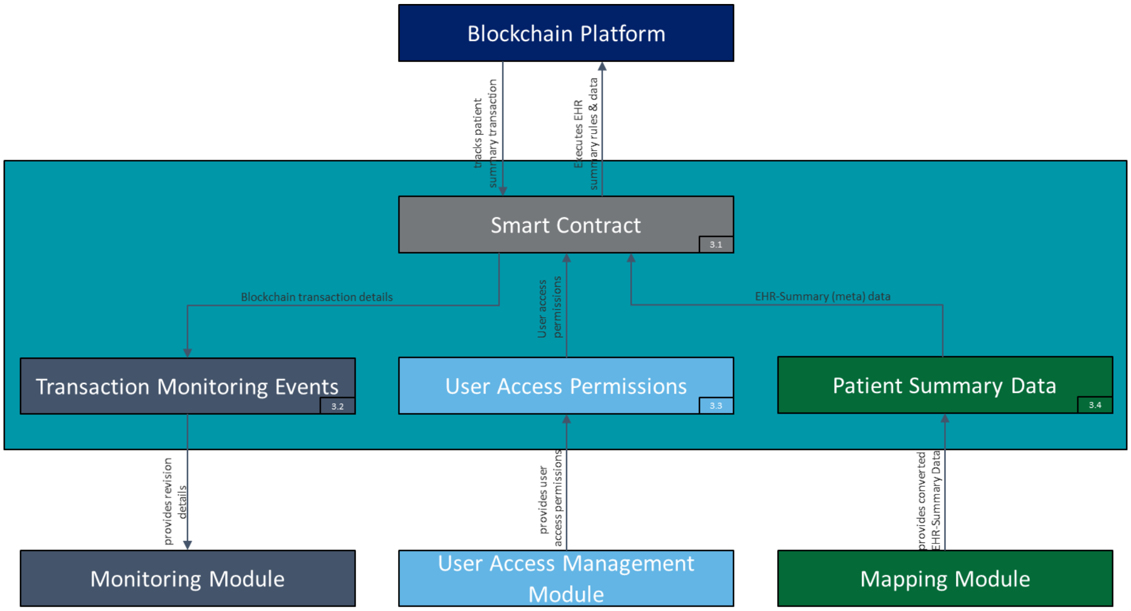

Blockchain Platform
tracks patient summary transaction
Executes EHR summary rules & data
Smart Contract
3.1
Blockchain transaction details
User access permissions
EHR-Summary (meta) data
Transaction Monitoring Events
3.2
User Access Permissions
3.3
Patient Summary Data
3.4
provides revision details
provides user access permissions
provides converted EHR-Summary Data
Monitoring Module
User Access Management Module
Mapping Module

Figure 12: Functional View - Smart Contract Module

The smart contract element acts as top-level entity within the module by combining the patient summary data with its related user access permissions which shall be hosted on to the Blockchain. In return the smart contract element tracks any transaction performed related to changes on the patient summary requested or executed by enforcing the defined user access permissions. This module is therefore the cornerstone of the proposed functional architecture by interacting directly with the Blockchain based on the prepared patient summary data, user access permissions and monitoring rules. Table 13 represents a summarised description of the smart contract module.

Element ID	Element Name	Element Description
3.1	Smart Contract	Enforces rules for: - Data hosted on Blockchain - User access permissions applied on Blockchain - Transactions performed/attempted on Blockchain
3.2	Transaction Monitoring Events	- Monitors transactions performed on Blockchain and issues alerts if needed
3.3	User Access Permissions	- provides user access permission according to the User Access Management Module
3.4	Patient Summary Data	- provides converted and created patient summary data to be hosted on Blockchain based on mapping module

Table 13: Description - Smart Contract Module

4.4 Informational Architecture

The informational architecture is according to Woods & Rozanski (2012) used to describe how the system stores, manipulates, manages and distributes information. The purpose of this chapter is therefore to represent a high-level view of the static data structure and information flow based on the proposed functional architecture.

Static Data Structure

The static data structure is used to represent the relations and dependencies among the data elements derived from the functional architecture. The static data structure represented in figure 13 describes the system by using the UML Class Model notation by displaying entities, their attributes and functions. Furthermore, the architecture documents the behavioural aspect of the system based on the relations between the entities according cardinalities defining how many instances of one entity can be related to another one as well as the visibility of the entities.

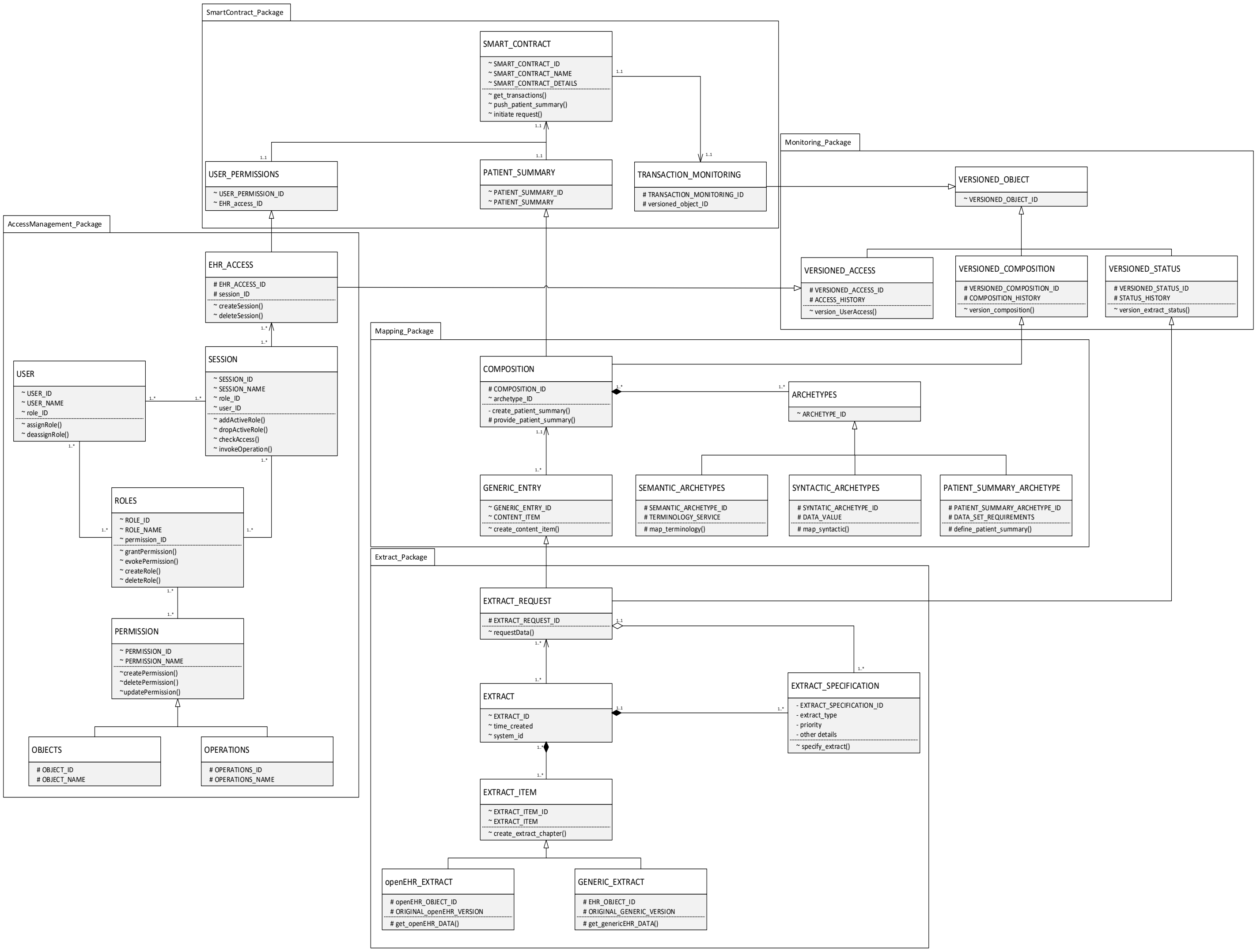


Figure 13: Informational Architecture - Static Data Structure

As it can be seen, the class model consists out of five packages based on the proposed functional architecture. In general, the class model has been designed without any public permissions assigned to the class attributes and functions. Reasons being related to security and modularity. Therefore, most of the attributes and functions are either assigned to protected (#) or packaged (~) visibility permissions. This shall assure that the attributes and functions described are only visible within the package or by its inherited class and cannot be seen nor called by other entities within the architecture.

The Extract_Package contains the classes responsible for extracting the patient data from various legacy systems which are either compliant to the openEHR reference model (*openEHR_EXTRACT* class) or any other data standard (*GENERIC_EXTRACT* class). The extract itself is specified by the *EXTRACT_SPECIFICATION* class, characterising the type (full or updated request), priority (low, medium or high priority) and other details such as the actual patient data being requested. The *EXTRACT* class entails meta data of the request such as the time of the launched request and if available, the legacy system_id. The *EXTRACT_REQUEST* class triggers the request within the package and is inherited by the *VERSIONED_STATUS* class of the Monitoring_Package in order to track the extract requests performed.

The Mapping_Package is responsible to convert the obtained data to a patient summary data set which can be uploaded to the Blockchain. The extracted data is therefore provided by the *GENERIC_ENTRY* class creating a content item per extract. The *COMPOSITION* class is the main instance for the conversion procedure which is controlled based on pre-defined archetypes to perform a syntactic and semantic mapping. Each composition created is logged by the *VERSIONED_COMPOSITION* class of the Monitoring_Package. Note that the mapping rules need to be defined for each data standard manually. According to the literature, the software platform "LinkEHR" would be a valuable tool in order to edit domain concepts, map EHR data to reference information models and archetypes and automatically create data transformation mechanisms (Maldonado et al., 2011). The result of the mapping procedure would be an XML file created based on the specified archetypes.

The AccessManagement_Package is in charge to specify the user access rights. Due to its role-based architecture, permissions can be created in a very granular fashion assuring that only the minimum required information is revealed. Important to note for this package is, that each user is assigned to one or more sessions to avoid potential segregation of duty violations. This is for instance important in the case when a practitioner switches the role from a healthcare record consumer to a healthcare record issuer (in case changes to the record are required). Note that the *EHR_ACCESS* class is the top instance of the package controlling the user sessions and potential changes made which are provided to the *VERSIONED_ACCESS* class of the Monitoring package.

The SmartContract_Package is considered as the interface to the Blockchain, capturing the specified user permissions and patient summary. Additionally, any related transaction made is monitored by the *TRANSACTION_MONITORING* class and provided to the Monitoring_Package.

Within the Monitoring_Package all transactions from the Blockchain are recorded and matched based on the predefined rules to identify potential violations in terms of changes and user access permissions. Furthermore, the Monitoring_Package oversees the whole data extraction and conversion process for medico-legal reasons. A detailed description of the class diagram and its attributes and functions can be found in Appendix O.

Information Flow

The information flow architectures is used to describe the dynamic movement of information between the elements of the proposed system. This perspective offers therefore the possibility to represent the data transferred from one component to another by taking the activities of the identified stakeholder into account (Woods & Rozanski, 2012). In order to represent the information flow properly, the BPMN 2.0 notation has been chosen. Reasons being, that the BPMN notation is readily understandable by all stakeholders representing end to end activities capable of including technical details. The BPMN diagram represented in figure 15, has therefore been designed for the main use-case of the provision of a patient summary on national and cross border level by consulting a healthcare provider. The diagram is divided into four lanes representing the activities of the stakeholder involved and starts with the activities represented by the patient. Those activities are in line with the described care pathway for the patient admission policy provided by the British National Health Service (Benson, 2005). As it can be seen the process starts by the patient who seeks care and consults a care provider. The care provider is responsible for the patient admission and launches a treatment request in the Patient Summary System. This treatment request contains important information such as the consultation date, consultation reasons and a consent that the patient agrees to receive care and allows therefore the system to obtain healthcare data from legacy system in order to consult or create a patient summary. Within the next step, the care provider being assigned to the role of the record consumer tries to access the patient summary. This activity is linked to a parallel task of the patient summary system by checking the user access permissions and availability of an existing patient summary. In case the record consumer is eligible of accessing the patient summary and the file is available, the system would provide the requested summary. In case no patient summary exists, the record consumer would need to switch its role to the healthcare record issuer and triggers the data extraction- and therefore the patient summary creation process. Once the patient summary has been created, the healthcare provider performs an initial screening of the patient to complete the summary with its basic data. Next, the patient receives the treatment by the healthcare provider. Once this has been completed, the patient gets discharged and the record issuer completes the treatment by documenting his work performed in the patient summary system. After this has been completed the patient receives a care notification by the patient summary system indicating the type of changes made to the healthcare record and has the possibility to acknowledge. As soon as this step has been completed, the patient summary system determines the changes made to the patient summary which would trigger a new transaction on the Blockchain.

A detailed description of the activities described within figure 14 can be found in table 15 below.

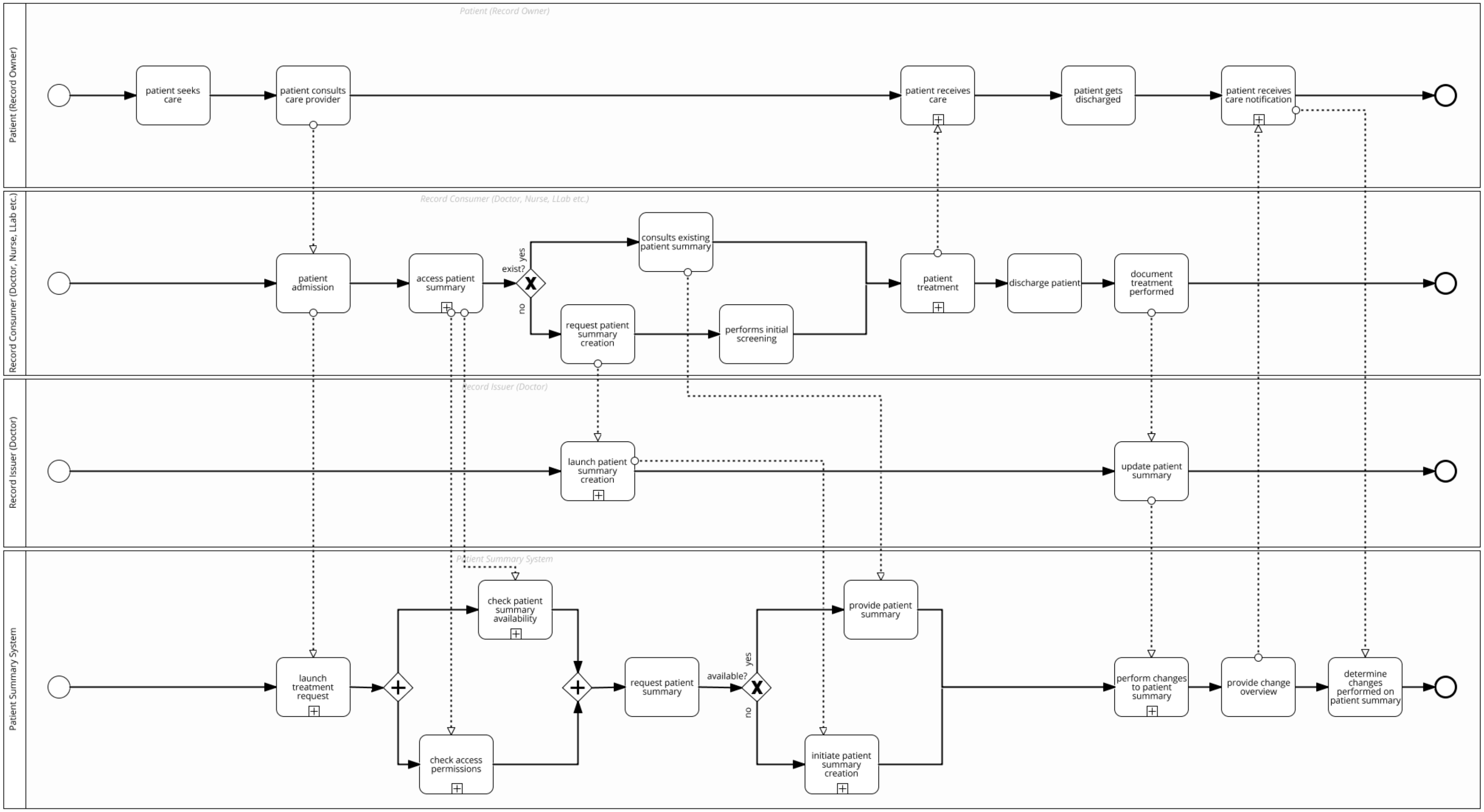

Patient (Record Owner)
Patient (Record Owner)
patient seeks care
patient consults care provider
patient receives care
patient gets discharged
patient receives care notification
Record Consumer (Doctor, Nurse, LLab etc.)
Record Consumer (Doctor, Nurse, LLab etc.)
patient admission
access patient summary
exist?
yes
no
consults existing patient summary
request patient summary creation
performs initial screening
patient treatment
discharge patient
document treatment performed
Record Issuer (Doctor)
Record Issuer (Doctor)
launch patient summary creation
update patient summary
Patient Summary System
Patient Summary System
launch treatment request
check patient summary availability
check access permissions
request patient summary
available?
yes
no
provide patient summary
initiate patient summary creation
perform changes to patient summary
provide change overview
determine changes performed on patient summary

Figure 14: Information Flow - BPMN Diagram

Lane	Element Name	Element Description
Patient	Patient seeks care	Task describing that the patient is in the need of care
Patient	Patient consults care provider	Task describing that the patient consults a healthcare provider to triggered based on the previous task.
Patient	Patient receives care	Task describing that the patient receives care form a healthcare provider. This could be an activity such as: - Evaluation (i.e. identification of allergies) - Instruction (i.e. describing the actions to perform in order to intervene - Action: type of observation corresponding to past, present and future - Observation: observing patient behaviour
Patient	Patients gets discharged	Completing the care consultation.
Patient	Patient receives care notification	Provision of a summary of changes performed based on the treatment received. Patient has the possibility to acknowledge to the changes made.
Record Consumer	Patient admission	Admission of the patient who consulted the care provider for care. Mostly done by nurse or care staff recording the time, date and reasons for consultation.
Record Consumer	Access patient summary	Task triggering to access the healthcare record
Record Consumer	XOR gateway: check patient summary existence	XOR gateway to determine if a patient summary already exist
Record Consumer	Consults existing patient summary	Consultation of an existing patient summary in order to determine the patient details.
Record Consumer	Request patient summary creation	Request to create a patient summary based on legacy data. Role from Record Consumer needs to be switched to Record Issuer to avoid a segregation of duty violation.
Record Consumer	Performs initial screening	Initial screening in order to complete the healthcare summary in case of incomplete data.
Record Consumer	Patient treatment	Treatment of the patient depending on the care request.
Record Consumer	Discharge patient	Completing the care treatment by discharging the patient.
Record Consumer	Documents treatment performed	Documenting the treatment performed of the patient visit in order to assure a complete patient history in the patient summary.
Record Issuer	Launch patient summary creation	Triggers the patient summary creation process based on the switched role of the record issuer.
Record Issuer	Update patient summary	Updates the patient summary according to the treatment performed.
Patient Summary System	Launch treatment request	Starts a session for a treatment by recording the basic details and providing consent, that the patient agrees to receive care and obtain historical patient data.
Patient Summary System	Check patient summary availability	Task performed by the monitoring model in order to assess if a patient summary has already been created within the past.
Patient Summary System	Check access permissions	Task performed in order to assure that the access is appropriate by the requestor.
Patient Summary System	Request patient summary	Task in order to request the patient summary
Patient Summary System	XOR gateway: checks patient summary availability	XOR gateway to determine if a patient summary already exist based on the result of task: check patient summary availability.
Patient Summary System	Provide patient summary	Provide patient summary as requested to the Record Consumer.
Patient Summary System	Initiate patient summary creation	Launches the extraction request in order to create a new patient summary.
Patient Summary System	Perform changes to patient summary	Performs changes to the patient summary depending on the treatment performed by record issuer.
Patient Summary System	Provide change overview	Provide overview of changes performed to the patient summary for the patient.
Patient Summary System	Determine changes performed on patient summary	Determine the changes performed based on an acknowledgement by the patient to send a request to the Blockchain.

Table 14: Description - Information Flow

5 Architecture Evaluation

Having described the design of the software architecture, this chapter focusses on the evaluation of the proposed system. As described earlier, an ATAM was applied to identify sensitivity points and trade-offs in order to answer sub-research question four and five. This was specifically done by exposing the architecture to scenarios in reference to each quality attribute (non-functional requirement). The next section describes the specific characteristics of each quality attribute. Followed by an analysis of the architecture by eliciting architectural decisions made. Finally, the third section describes the evaluation of the architecture from the stakeholder perspective which has been conducted throughout a workshop session in line with step seven and eight of the ATAM. Note that the architecture has been evaluated for the two identified Blockchains types of permissioned and permission-less systems. For permission-less environments Ethereum has been chosen due to the possibility to execute smart contracts in permission-less environments, being the first solution available after the Bitcoin Blockchain and having the second biggest market capitalisation. For permissioned environments Hyperledger Sawtooth has been chosen due to its on-chain governance, advanced transaction execution engine and optimisation in terms of consensus mechanisms for healthcare related solutions.

5.1 ATAM – Presentation

According to the literature, the achievement of quality attributes is critical for the success of a software system. In order to evaluate a software architecture properly, it is therefore crucial to define those quality attributes thoroughly. System specific scenarios can support the description of those quality attributes (Barbacci et al., 2003; BinSubaih & Maddock, 2006). As described in chapter 4, non-functional requirements can be considered as quality attributes. The proposed architecture was therefore evaluated for the quality attributes of: security & privacy, performance, communication, medico-legal and evaluation which have been obtained from the ISO 18308 standard mentioned in chapter 2.

Quality Attributes – Communication

ID	Attribute category	Attribute description
ME1	Messaging	The EHR must support the export and import of data received using messaging protocols such as HL7, UN/EDIFACT and DICOM.
RE1	Record Exchange	The EHR must allow for the exchange of a complete EHR or a part of an EHR (an extract) between EHR compliant systems.
RE2		The EHR must support serialisation of data for interoperability purposes (e.g. via XML, CORBA, SOAP, etc.).
RE3		The EHR must define the semantics of merging data from an EHR extract with the EHR resident in the receiving system.
RE4		The EHR must provide an audit trail of exchange processes, including authentication, to enable identification of points of EHR extract transmittal and receipt.
RE5		The rules covering the exchange of an extract must be the same as those for exchanging the complete record.
RE6		The EHR must enable semantic interoperability of clinical concepts between EHR systems to support automatic processing of data at the receiving system.

Table 15: Quality Attributes - Communication

Quality Attributes – Security & Privacy

ID	Attribute category	Attribute description
PC1	Privacy and confidentiality	The EHR must support the application of prevailing privacy and confidentiality rules.
PC2		The EHR must support the labelling of the whole and/or sections of the EHR as restricted to authorised users and/or purposes. This should include restrictions at the level of reading, writing, amendment, verification, and transmission/disclosure of data and records
PC3		The EHR must support privacy and confidentiality restrictions at the level of both data sets and discrete data attributes.
C1	Consent	The EHR must support recording of informed consent for the creation of a record.
C2		The EHR must support obtaining, recording and tracking the status of informed consent to access the whole and/or sections of the EHR, for defined purposes.
C3		The EHR must support recording of the purposes for which consent is obtained.
C4		The EHR must support recording of the time frames attached to each consent.
AC1	Access Controls	The EHR must support measures to define, attach, modify and remove access rights to the whole and/or sections of the EHR.
AC2		The EHR must support measures to define, attach, modify and remove access rights for classes of users of the EHR.
AC3		The EHR must support measures to enable and restrict access to the whole and/or sections of the EHR in accordance with prevailing consent and access rules.
AC4		The EHR must support measures to separately control authorities to add to and/or modify the EHR from authorities to access the HER.
DI1	Data Integrity	The EHR must support measures to ensure the integrity of data stored in and transferred to and from EHRs
AA1	Auditability of access	The EHR must support recording of an audit trail of access to and modifications of data within the whole or sections of the EHR.
AA2		The EHR must support recording of the nature of each access and/or transaction.
AA3		The EHR must support audit capability sufficient to track accountability for each step or task in the clinical or operational processes recorded in the record.

Table 16: Quality Attributes - Security & Privacy

Quality Attributes - Performance

The scalability requirement suggested by the ISO 18308 is defined as follows: *"The EHR should not impede efficient processing of very large records or very large numbers of records.".* This is in terms of transaction throughput and latency rather vaguely defined and difficult to evaluate. The following assumption has therefore been made to determine the desired transaction throughput and latency. Given the use case described within the information flow and class diagram, approximately 30 transactions need to be executed per patient admission (identified based on activities and functions declared). According to the general hospitals branch report for the Netherlands, on average, 1.69 million patients were seeking care on an annual basis (between 2008 – 2012) (Lee, 2013) which has been used as a base to calculate the transaction throughput.

ID	Attribute category	Attribute description
T1	Transaction throughput	The EHR system must offer a minimum transaction throughput of approximately 2 transactions per second. (The transaction throughput has been calculated by multiplying the hospital admissions (1.69 mil) with the assumed transactions (30), divided by seconds per year (31536000). In short: (1690000 x 30)/31536000 ≈ 1.60 tp/s)).
L1	Latency	The latency depends on the size of data send throughout the network. According to (Lee, 2015) a latency between 0.1s – 1s can be considered as acceptable.

Table 17: Quality Attributes – Performance

Quality Attributes – Evolution

ID	Attribute category	Attribute description
EV1	Support for EHR architecture and EHR system evolution	Backwards compatibility of EHR software: Any implementation of the EHR must be able to process EHRs created under older versions of the EHR.
EV2		Backwards compatibility of the EHR: Software built on a previous version of the EHR must be capable of processing EHRs created under a newer version of the EHR.
EV3		The EHR must be able to accommodate the recording of information due to new forms of clinical knowledge, new clinical disciplines, and new clinical practices and processes.

Table 18: Quality Attributes - Evolution

Quality Attributes - Medico-Legal

ID	Attribute category	Attribute description
SR1	Support for legal requirements	The EHR must support measures to ensure an accurate reflection of the chronology of clinical events and information availability in the EHR.
SH1	Subject of healthcare	The EHR must cater for the subject of care of the EHR to be one or more persons.
PID1	Patient identification	The EHR must cater for the recording of appropriate patient identification attributes and clinically relevant patient attributes such as date of birth, sex, ethnicity etc.
UI1	User Identification	The EHR must ensure that users who attest and commit any particular information to the record are uniquely and reliably identified.
UI2		The EHR must support the on-going ability to identify users, even if they change their name, profession, sex, or address.
HP1	Healthcare parties	The EHR must support measures to ensure that all clinical parties referred to in the HER are uniquely identified.
HP2		The EHR must support the recording of the clinical roles of any parties with respect to any clinical activity recorded.
AR1	Author responsibility	The EHR must support measures which ensure that every record entry is dated, its author identified.
AR2		The EHR must support measures to ensure that there is an absolute requirement that each contribution to the record is attributed to a responsible healthcare party whether in the role of author or not.
AE1	Attestation/Authorisation of entries	The EHR must support measures which ensure that every contribution to the record must be attested by a responsible person.
AE2		The EHR must support measures which ensure that amendments are attributed to a responsible person and the date and time and the reason for the amendment are recorded.
CG1	Clinical competence/governance	The EHR must support the demonstration of clinical competence and accountability of clinicians.
FA1	Faithfulness	The EHR must ensure that information intended to supersede that already recorded and attested must be separately collected and attested as a new transaction version.
FA2		The EHR must ensure that the exact state of the record can be re-created for any given point of time since the original creation of the EHR.
PC1	Preservation of context	Where coded terms in the EHR have been mapped to another coded terminology, the EHR must provide a means of indicating the faithfulness of the translation.
PC2		The EHR must maintain the original context of all elements of the record irrespective of the potential separate distribution of elements.
PE1	Permanence	The EHR must ensure that attested information shall be stored in a protected mode, disallowing any changes or deletions.
PE2		The EHR will ensure that amendments are attributed to a clinician and the date and time, and the reason for the amendment are recorded.
VC1	Version control	The EHR must incorporate a method of version control that supports information at the level at which it was attested.
VC2		The EHR must support measures to discern modification or updating of the record using version control.

Table 19: Quality Attributes - Medico-Legal

5.2 ATAM – Analysis

As mentioned before, the architectures success is dependent on the architectural decisions made to achieve the identified quality attributes. The section below describes the architecture decisions made per quality attribute described earlier.

Architectural Decisions to Support the Communication Quality Attribute:

For the communication quality attribute, the architect made four decisions in order to achieve the quality attribute.

AD1: openEHR archetypes

The first architectural decision is the corner-stone of the whole architecture by taking advantage of the openEHR reference model. Due to the fact, that the openEHR reference model is compliant with other standards such as HL7, data from any other source can be incorporated and represented within the proposed system in native openEHR form as long as a mapping is performed. This could be in any serialisation mechanism such as XML or JSON. Furthermore, offers the framework the possibility to represent data which is unable to be converted in an encapsulated form.

AD2: extract module

The extract module has been designed in order to assure a complete data transfer from various legacy systems which are either compliant with the openEHR framework or represent any other form. Important to note is that extract queries need to be predefined for non-openEHR systems.

AD3: monitoring module

The monitoring module shall support the communication process for two things. First, by specifying the request for the target system and second, by monitoring the extraction process from the audit perspective, specifically based on the VERSIONED_STATUS class. This is also related to medico-legal requirements.

AD4: mapping module

The mapping module makes use of openEHR archetypes in order to convert the data obtained from various legacy systems into an openEHR compliant form. Due to the fact that three classes are responsible for the syntactic- and semantic mapping as well as for the creation of the patient summary, semantic interoperability shall be achieved. Note, that the mapping and conversion rules need to be pre-defined in advance for a proper conversion.

Architectural Decisions to Support Security & Privacy Quality Attributes:

Regarding to the security & privacy quality attribute, two architectural decisions have been made which are described below.

AD5: role-based access control system

The access management package has been designed in a way to enforce granular user access permissions allowing a temporary activation of specific access rights through user sessions. Based on this design, it is possible to control user access permissions by a central instance allowing access limitations for specific sections of the patient summary depending of the assigned role. This design enforces therefore privacy and confidentiality rules.

AD6: limited attributed visibility

Assigning limited attribute visibility to the architecture shall assure that class related functions and attributes are only executable from the dedicated module and not from another instance i.e. triggering a request without permissions or specifications.

Architectural Decisions to Support Performance Quality Attributes:

No specific architectural decisions regarding to the performance have been made at the design stage for the functional and informational view. Reasons being, that this quality attribute can only be assessed based on real requests exposed to the architecture. In order to assess this quality attribute, known performance specifications for permissioned and permission-less blockchain systems were analysed later in the chapter.

Architectural Decisions to Support Evolution Quality Attributes:

As described earlier, the decisions to make use of the openEHR reference model (AD1) within the proposed architecture shall support the overall system evolution. The two-level modelling approach satisfies therefore the requirement of covering and defining old and new business rules. For example, if a new use-case shall be applied within the architecture such as the achievement of ePrescriptions on national and cross-border level, as mentioned within the eHealth Stakeholder (2014), a new archetype would need to be developed which can be integrated into the existing architecture.

Architectural Decisions to Support Medico-Legal Quality Attributes:

Concerning the achievement of the medico-legal quality attributes a various architectural decisions have been made which have been partly described earlier. Important for this quality attribute is that the content kept on the system is trusted by all stakeholders involved and accepted in courts of law as evidence of care provided. The medico-legal requirements are therefore mostly related to security and privacy concerns. Two distinct architectural decisions have been made regarding the achievement of medico-legal quality attributes described below.

AD7: transaction monitoring

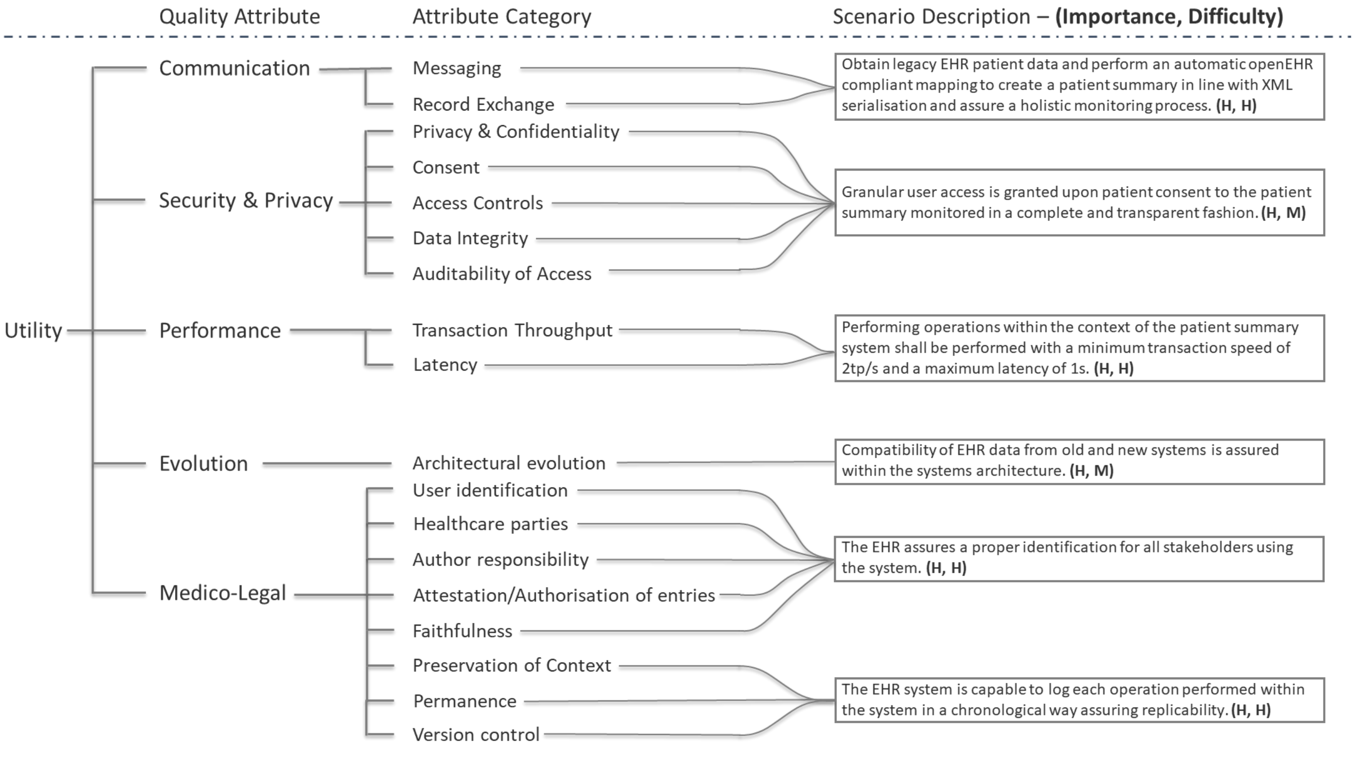
The decision to integrate an element responsible for the transaction monitoring performed on the blockchain is necessary in order to identify potential violations of the rules applied. The class *TRANSACTION_MONITORING* provides therefore the data of changes (transactions) performed to the patient summary in order assure that those were in line with the defined access rules and archetypes.

AD8: patient summary archetype

The patient data archetype is the element representing the clinical data of the patient seeking care. Within this archetype the basic clinical data required for patient summary is defined on syntactical and semantical level which is hosted on the Blockchain. Any change made to the archetype and to the summary itself can be monitored and adjusted according to the desired use-access permissions. This shall assure that medico-legal requirements are met.

Utility Tree

The purpose of the utility tree is to elicit the quality attributes down into practical scenarios. This shall aid the evaluation in case the quality attributes are defined in an unambigous manner. Additionally, aids the utility tree to prioritise the scenarios which shall streamline the evaluation process to address the most important quality attributes. The utility tree represented in figure 15 is based on three levels. The last level holds the scenarios created based on the requirements described within the ISO18308. According to BinSubaih & Maddock (2006) are the benefits of describing quality attributes based on scenarios threefold: first, they are simple to create and understand, second it is an inexpensive process and third, they are an effective way to validate an architecture. Furthermore represents the last level of the utility tree a relative attribute ranking from High (H), Medium (M), and Low (L) for the variables of importance and difficulty. The importance variable states how substantial the achievement of the quality attribute is for the success of the architecture and the difficulty describes the degree complexity in achieving this quality attribute. The prioritisation has been done based on professional judgement by the architect who developed the architecture according to the use-case scenarios described earlier in reference to the challenges identified throughout the SLR.



Obtain legacy EHR patient data and perform an automatic openEHR compliant mapping to create a patient summary in line with XML serialisation and assure a holistic monitoring process. **(H, H)**

Granular user access is granted upon patient consent to the patient summary monitored in a complete and transparent fashion. **(H, M)**

Performing operations within the context of the patient summary system shall be performed with a minimum transaction speed of 2tp/s and a maximum latency of 1s. **(H, H)**

Compatibility of EHR data from old and new systems is assured within the systems architecture. **(H, M)**

The EHR assures a proper identification for all stakeholders using the system. **(H, H)**

The EHR system is capable to log each operation performed within the system in a chronological way assuring replicability. **(H, H)**

Figure 15: Utility Tree

Analysis of Architectural Approaches

Having created the utility tree, this section analysis the architectural decisions made to determine how well they correlate to the defined quality attributes and if those are satisfied by the designed architecture. The result of this chapter is a detailed description regarding to the architectural decisions made by revealing sensitivities, trade-offs, risks and non-risks. Within the context of the ATAM, a risk is considered as a weakness within the architecture unable to support a prioritised quality attribute. A non-risk can be considered as a strength of the architecture fulfilling the prioritised quality attribute. Sensitivities characterise one or more components for the achievement of the given quality attribute. In case the architecture is sensitive at a point for more than one attribute, the point is considered as a trade-off. According to Kazman, Klein, & Clements (2000) is the examination level not meant to be comprehensive and detailed but rather commensurate with regards to the architectural requirements requiring engineering judgement by the architect. Important for this phase is to establish a link between the architectural decision and the quality attributes which shall be satisfied. The tables below describe the examiniation per quality attribute in reference to the architectural decision based on the generated scenarios earlier followed by a description of the sensitivities, trade-offs, risks and non-risks. Note that the scenarios are described following a three part format: stimulus, environment and response. The stimulus describes what initiated an interaction with the architecture. The environment describes the state of the architecture when the interaction takes place and the response explains how the architecture reacts to the interaction (BinSubaih & Maddock, 2006).

Due to the fact that the same sensitivities, trade-offs, risks and non-risks can be applicable for different scenarios, an identification scheme has been used to avoid redundancies in the documentation and to point out recurring characteristics important for a variety of quality attributes. The identification scheme is defined as followed:

- First item: reference to the quality attribute (C = Communicate, SP = Security & Privacy, P = Performance, E = Evolution & ML = Medico-Legal)
- Second item: reference to the architectural characteristic (S = Sensitivity, T = Trade-Off, R = Risk, N = Non-risk)
- Third item: reference to to architectural decision
- Fourth item: sequential numbering in case of multiple items applicable for one architectural design

As an example, the ID: C-S2b refers therefore to the quality attribute “Communication” with the characteristic of a “Sensitivity” related to the second “Architectural Decisions” for which it is the second item.

Examination: Communication Quality Attribute

Analysing Attribute	**Communication**			
Scenario	Obtain legacy EHR patient data and perform an automatic openEHR compliant mapping to create a patient summary in line with XML serialisation and assure a holistic monitoring process.			
Quality Attribute	Messaging & Record Exchange			
Stimulus	Patient seeks care and Healthcare record consumer/issuer requests access to patient summary.			
Environment	Patient summary system checks permissions and patient summary availability.			
Response	Patient summary system obtains patient summary data (ETL), provides patient summary and logs all operations performed.			
Architecture Decision	**Sensitivity**	**Trade-off**	**Risk**	**Non-risk**
AD1	C-S1a	C-T1a	C-R1a	C-N1a, C-N1b
AD2	C-S2a, C-S2b	C-T2a, C-T2b	C-R2a, C-R2b	C-N1a
AD3	C-S2a	C-T2a	C-R2a	C-N3a
AD4	C-S4a	C-T4a	C-R4a, C-R2b	
AD5	C-S5a	C-T5a	C-R5a	C-N5a, C-N5b
AD6				
AD7	C-S7a	C-T7a	C-R7a	C-N7a
AD8	C-S8a	C-T8a	C-R8a	

Table 20: Examination Results - Quality Attribute: Communication

Sensitivity Points	
C-S1	suspended support for openEHR reference mode
C-S2a	concerns over message/data load
C-S2b	concerns over legacy system identification/authorisation possibilities
C-S4a	concerns over the complexity to create accurate mapping rules
C-S5a	concerns over complexity to create proper user access management rules
C-S7a	concerns over transaction speed from Blockchain platform and processing capabilities of the patient summary system
C-S8a	concerns over level of security in pre-processing patient summary system and summary hosted on a permission-less blockchain
Trade-Offs	
C-T1a	Communication (+), Medico-Legal (+) vs. Evolution (-)
C-T2a	Communication (+) vs. Performance (-)
C-T2b	Communication (+) vs. Medico-Legal (-)
C-T4a	Communication (+) vs. Performance (-), Medico-Legal (-)
C-T5a	Communication (+) vs. Security & Privacy (-)
C-T7a	Communication (+), Medico-Legal (+), Security & Privacy (+) vs. Performance (-)
C-T8a	Communication (+) vs. Security & Privacy (-), Medico-Legal (-)
Risks	
C-R1a	architectural evaluation/continuity is at risk in case of dispensed openEHR support
C-R2a	violation of national/international laws and compliance to obtain patient data
C-R2b	potential heavy workload on both, legacy and patient summary system
C-R4a	altered data/data integrity
C-R5a	not appropriate defined & enforced user access rights, hence possible lack of accountability
C-R7a	increased latency due to increased message workload within the patient summary system independent if permissioned or permission-less system is being used (permissioned systems would be more beneficial due to performance advantage)
C-R8a	In case the patient summary is hosted on a permission-less blockchain, it is inexplicable which nodes host the patient summary which might lead to security flaws and violations of national laws (By the time of this study, the legal situation is unclear how to proceed with data ownership and accessibility related questions within the case of a Blockchain.)
Non-Risks	
C-N1a	communication among non- and openEHR compliant systems is assured due to openEHR reference model
C-N1b	transferability of created openEHR archetypes to other ontologies is assured due to meta-modelling approach
C-N3a	all operations being recorded in a serialised manner (i.e. XML, JSON, .NET) within the patient summary system
C-N5a	granular user access management can be assured due to RBAC module
C-N7a	Auditability and traceability is thoroughly assured within the system

Table 21: Examination Details - Quality Attribute: Communication

Examination: Security & Privacy Quality Attribute

Analysing Attribute	**Security & Privacy**			
Scenario	Granular user access is granted upon patient consent to the patient summary monitored in a complete and transparent fashion.			
Quality Attribute	Privacy, Confidentiality, Access Control, Data Integrity & Auditability Access			
Stimulus	User requests access to specific part of the system (i.e. patient summary, monitoring module, smart contract)			
Environment	Patient summary systems checks if access request is appropriate			
Response	Patient summary grants or denies access request			
Architecture Decision	**Sensitivity**	**Trade-off**	**Risk**	**Non-risk**
AD1				
AD2				
AD3	SP-S3a		SP-R3a	
AD4				
AD5	C-S5a	C-T5a	C-R5a	C-N5a, C-N5b
AD6				
AD7	C-S7a	C-T7a	C-R7a	C-N7a
AD8				

Table 22: Examination Results - Quality Attribute: Security & Privacy

Sensitivity Points	
SP-S3a	Concerns regarding the proper identification of user access violations
Risks	
SP-R3a	Unable to identify user access violations due to weakly defined user access rights leading to a lack of accountability

Table 23: Examination Details - Quality Attribute: Security & Privacy

Examination: Performance Quality Attribute

Analysing Attribute	**Performance**			
Attribute Description	Performing operations within the context of the patient summary system shall be performed with a minimum transaction speed of 2tp/s and a maximum latency of 1s.			
Quality Attribute	Transaction throughput, Latency			
Stimulus	Transaction is issued to the patient summary system.			
Environment	Transaction is processed by the system (either from summary system or Blockchain).			
Response	Transaction is settled and completed below 1s of latency.			
Architecture Decision	**Sensitivity**	**Trade-off**	**Risk**	**Non-risk**
AD1				
AD2	P-S2a, P-S2b	P-T2b	P-R2a	P-N2b
AD3	P-S3a, C-S2a	C-T3a	C-R3a	P-N3a
AD4	P-S2a P-S2b	P-T2b	P-R2a	P-N2b
AD5				
AD6				
AD7	P-S7a P-S7b	P-T7a P-T7b	P-R7a P-R7b	P-N7a P-N7b
AD8				

Table 24: Examination Results - Quality Attribute: Performance

Sensitivity Points	
P-S2a	Security concerns since a permission-less environment would need to interact with an interface between the blockchain and the preliminary system.
P-S2b	Performance concerns to extract data from legacy systems independent if a permissioned or permission-less Blockchain is used.
P-S3a	Concerns regarding the message load and the creation of a bottleneck due to the dependency of AD7.
P-S7a	Major performance concerns due to node dependency and distributed characteristic for permission-less environments.
P-S7b	Security concerns due to limited number of nodes and central unit to assign permissions for permissioned environments.
Trade-Offs	
P-T2b	Security & Privacy (+) & Medico-Legal (+) vs. Performance (-) - (concerning permissioned Blockchain environments)
P-T7a	Security & privacy (+), Medico-Legal (+), Communication (+) vs. Performance (-) - (concerning permission-less environments)
P-T7b	Performance (+) vs. Security & Privacy (-) - (concerning permissioned environments)

Risks	
P-R2a	Data integrity due to malicious intents such as spoofing to obtain extracted data
P-R3a	Clogged system due to dependency of network nodes
P-R7a	Potential network breakdown due to note dependencies
P-R7b	Thread of exposed consensus mechanism due to limited number of nodes
P-R9a	Risk of facing a network breakdown due to note dependency for permission-less environments
P-R9b	Risk of exposing the consensus mechanism due to limited number of nodes
Non-Risks	
P-N2b	Stability of the system to act an integrated manner (concerning permissioned environments)
P-N3a	Avoidance of a clogged system due to node stability (concerning permissioned environments)
P-N7a	Almost inherent level of security (data integrity) inherent to permission-less architecture (concerning permission-less environments)
P-N7b	System performance reliability (concerning permissioned environments)

Table 25: Examination Details - Quality Attribute: Performance

Examination: Evolution Quality Attribute

Analysing Attribute	**Evolution**			
Attribute Description	Compatibility of EHR data from old and new systems is assured within the systems architecture.			
Quality Attribute	Architectural evolution			
Stimulus	Changes to the systems architecture due to external requirements (i.e. medico-legal reasons).			
Environment	Default system architecture.			
Response	Adapted system architecture.			
Architecture Decision	**Sensitivity**	**Trade-off**	**Risk**	**Non-risk**
AD1	C-S1a	C-T1a	C-R1a	C-N1a C-N1b
AD2				
AD3				
AD4	E-S4a	E-T4a	E-R4a	E-N4a
AD5				E-N5a
AD6	E-S6a		E-R6a	
AD7				
AD8				

Table 26: Examination Results - Quality Attribute: Evolution

Sensitivity Points	
E-S4a	Concern in terms of new/old mapping rules which have to be adapted according to the new requirements
E-S7a	Concerns of the system applicability to deal with changes to its current architecture
Trade-Offs	
E-T4a	Evolution (+) vs. Communication (-)
E-T6a	Security & Privacy (+) vs. Evolution (-) & Communication (-)
Risks	
E-R4a	The system might be incapable of handling the new requirements due to limitations in the architecture which are not visible at this development stage
E-R7a	Inflexibility of the system due to its attribute & class limitations
Non-Risks	
E-N4a	Modularity of the system and the use of openEHR shall assure the possibility to adapt the system depending of its circumstances
E-N5a	Flexibility of the system to deal with new user requirements

Table 27: Examination Details - Quality Attribute: Evolution

Examination: Medico-Legal Quality Attribute

Analysing Attribute	**Medico-Legal**			
Attribute Description	The EHR assures a proper identification for all stakeholders using the system in a permanent way.			
Quality Attribute	User identification, healthcare parties, author responsibility, attestation/authorisation of entries, faithfulness			
Stimulus	Stakeholder attempts to access specific part within the system.			
Environment	System assesses user access permissions.			
Response	System grants or denies access and logs the attempts in a permanent manner.			
Architecture Decision	**Sensitivity**	**Trade-off**	**Risk**	**Non-risk**
AD1				ML-N1a
AD2				
AD3				ML-N3a
AD4				
AD5	C-S5a	C-T5a	C-R5a	C-N5a, C-N5b
AD6				
AD7				
AD8				

Table 28: Examination Results - Quality Attribute: Medico-Legal (I)

Non-Risks	
ML-N1a	Predefined openEHR archetypes support the identification of any subject trying to access the system which is enforced via. AD5
ML-N3a	Attestation of operations performed within the system can be assured thoroughly

Table 29: Examination Details - Quality Attribute: Medico-Legal (I)

Analysing Attribute	**Medico-Legal**			
Attribute Description	The EHR system is capable to log each operation performed within the system in a chronological way assuring replicability.			
Quality Attribute	Preservation of context, permanence & version control			
Stimulus	Operation is performed within the system.			
Environment	System oversees operations performed.			
Response	System issues an alert to the dedicated user.			
Architecture Decision	**Sensitivity**	**Trade-off**	**Risk**	**Non-risk**
AD1	C-S1a	C-T1a	C-R1a	C-N1a, C-N1b
AD2	C-S2a	C-T2a	C-R2b	C-N2a
AD3	C-S2a	C-T2a	C-R2b	C-N2a
AD4				
AD5				
AD6				
AD7	ML-S7a	ML-T7a	ML-R7a	
AD8				

Table 30: Examination Results - Quality Attribute: Medico-Legal (II)

Sensitivity Points	
ML-S7a	Concerns if transactions monitored from the blockchain are relevant
Trade-Offs	
ML-T7a	Medico-Legal (+) vs. Communication (-) & Performance (-)
Risks	
ML-R7a	System not able to sift out relevant transactions for its monitoring procedures

Table 31: Examination Details - Quality Attribute: Medico-Legal (II)

5.3 ATAM – Testing

The testing phase of the ATAM consists of two steps. First, brainstorming and prioritising scenarios (ATAM step 7), and second, analysing the architectural decisions based on the generated scenarios during the brainstorming (ATAM step 8, similar to the analysis of architectural approaches described in the previous section). In comparison to the scenarios reflected in the utility tree, the objective for this phase is to widen the spectrum of scenarios the software architecture is likely to encounter by involving its stakeholders. This approach can be described as a bottom-up approach, whereas the examination based on the utility tree is considered as top-down approach (BinSubaih & Maddock, 2006).

5 participants were involved in the first step of the testing phase with a proven track-record in the areas of healthcare, Distributed Ledger Technologies, Data Science and Software Architecture engineering being partially knowledgeable about the research topic and representatives of the stakeholders identified earlier. The participants were expected to brainstorm the following three kinds of scenarios:

- Use case scenario: representing ways in which the stakeholder expects the system to behave from the end-user perspective.
- Growth scenario: representing ways in which the stakeholder expects the system to change in the future.
- Exploratory scenario: representing ways in which the stakeholder expects the system to change in extreme forms of growth i.e. dramatic new performance or medico-legal requirements.

After the brainstorming, the generated scenarios were collected, merged (in case of a mutual quality attribute) and prioritized according to a voting scheme. The number of votes allocated for each participant was 30% based on the total number of scenarios generated. This percentage is recommended by the guidelines provided Kazman et al. (2000). The weight of the scenarios was entirely defined by the participants having the liberty to allocate their votes in any way they considered the scenarios as most important. For example, they could assign all their votes to one scenario or distribute them equally among the scenarios. After the voting, the highest ranked scenarios were identified by selecting them based on the majority of votes received. As a final step, the selected scenarios were compared to the prioritized scenarios obtained from the utility tree in step 5, placed under the appropriate branch and analysed to identify further sensitivities, trade-offs, risks and non-risks of the architecture.

Scenario Brainstorming and Priorisation

In order to assure that the participants understood the research background and workshop objective, a thorough introduction was given by the architect. After, the brainstorming session was performed in five rounds according to the round-robin principle assuring, that each participant had the chance to generate five scenarios inspired by ideas of the remaining participants. As a result, 25 scenarios could be collected (see appendix P for a full scenario list). According to the described 30% voting distribution rule, each participant received 8 votes to prioritise the generated scenarios. Figure 16 represents the distribution of votes received per scenario indicating, that the three scenarios above the cut-off line of 3.5 received the majority of votes and have been therefore selected for the analysis. Table 16 describes the selected scenarios.

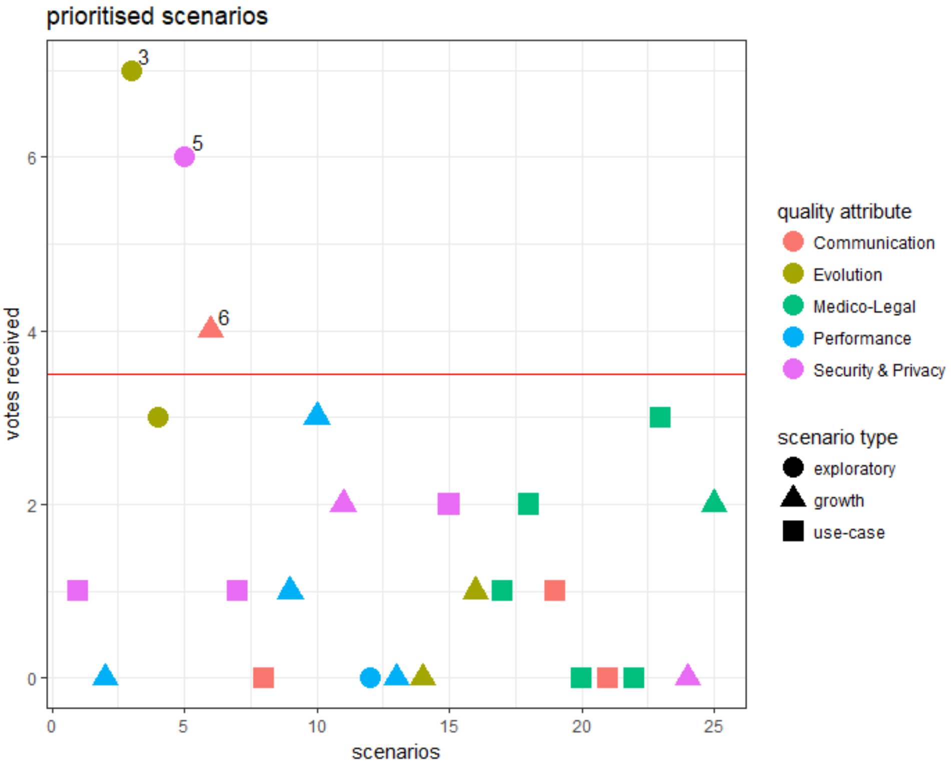


Figure 16: Prioritised Scenarios

#	Scenario	quality attribute	scenario type	received votes
3	The Blockchain protocol becomes outdated or obsolete. A new one is needed, and it should be possible to do this transition relatively smooth.	Evolution	Exploratory	7
5	The encryption keys are lost, potentially all data is lost.	Security & Privacy	Exploratory	6
6	Once a new system/hospital/country wants to use the architecture it should be possible to integrate them easily within short time.	Communication	Growth	4

Table 32: Selected High Priority Scenarios

Analysis of Brainstormed Scenarios

Having collected and prioritised the scenarios from the workshop, the scenarios have been analysed the same way as described in chapter 5.2 The section below provides therefore two tables per scenario representing details regarding identified sensitivities, trade-offs, risks and non-risks.

Note that the third scenario identified by the stakeholders described as follows: *“Once a new system/hospital/country wants to use the architecture it should be possible to integrate them easily within short time.”* has already been considered within the analysis with respect to the communication quality attribute. An analysis of potential sensitivity points, trade-offs, risks and non-risks was therefore obsolete; yet emphasizes the expectations in terms of flexibility of the system. The details for this analysis for the third scenario are reflected within table 34 & 36.

Examination: first priority scenario identified based on stakeholder brainstorming

Analysing Attribute	**Evolution**			
Attribute Description	The Blockchain protocol becomes outdated or obsolete. A new one is needed, and it should be possible to do this transition relatively smooth.			
Quality Attribute	Architectural evolution			
Stimulus	The Blockchain protocol the system is based on reaches its end-of-life point.			
Environment	The architecture is going to be migrated to a new Blockchain protocol.			
Response	The architecture runs under a new Blockchain protocol			
Architecture Decision	**Sensitivity**	**Trade-off**	**Risk**	**Non-risk**
AD1				E-N1a
AD2				
AD3				
AD4				E-N4b
AD5				
AD6				
AD7	E-S7a		E-R7a	
AD8				

Table 33: Examination Results - Quality Attribute: Evolution (II)

Sensitivity Points	
E-S7a	Concerns over the adaptability and migration approach towards the new Blockchain protocol.
Risks	
E-R7a	In case the new Blockchain protocol is incapable to meet the requirements of the system, a risk in terms of business continuity arises.
Non-Risks	
E-N1a	The change towards a new protocol will have no impact on the openEHR reference model. The architecture is therefore capable of being applied on different kind of Blockchains as long as they are capable of dealing with smart contracts according to the defined requirements.
E-N4b	Due to the fact, that records written on the Blockchain are considered as tamper-proof, previously recorded data is still available and accessible. In case a new protocol is needed, a (soft/hard-) fork of the nodes could help to switch to the new protocol whereas the old one is still accessible.

Table 34: Examination Details - Quality Attribute: Evolution (II)

Examination: second priority scenario identified based on stakeholder brainstorming

Analysing Attribute	**Security & Privacy**			
Attribute Description	The encryption keys are lost, potentially all data is lost/not accessible.			
Quality Attribute	Authorisation			
Stimulus	Access to the healthcare record is requested without having the private keys to access the data on the Blockchain.			
Environment	The system denies the access to the data without having appropriate authorisation rights.			
Response	The access request will be denied.			
Architecture Decision	**Sensitivity**	**Trade-off**	**Risk**	**Non-risk**
AD1				
AD2				
AD3	SP-S3b	SP-T3a		SP-N3a
AD4				
AD5	SP-S5a	SP-T5a	SP-R5a	SP-N5a, SP-N5b, SP-N5c
AD6				
AD7				
AD8				

Table 35: Examination Results - Quality Attribute: Security & Privacy (II)

Sensitivity Points	
SP-S3b	Concerns over the monitoring rules applied for data which is not accessible anymore.
SP-S5a	Concerns over future-proven authorisation mechanisms.
Trade-Offs	
SP-T3b	Medico-Legal (+) vs. Security & Privacy (-)
SP-T5a	Security & Privacy (+) vs. Communication (-)
Risks	
SP-R5a	Data hosted on the Blockchain will not be accessible without appropriate and available authorisation mechanisms.
Non-Risks	
SP-N3b	Even if the data is not accessible, the patient data is still monitored by the monitoring agent.
SP-N5a	Data can be recreated in case it is not accessible.
SP-N5b	Data is not accessible and therefore also protected against unauthorised access.
SP-N5c	Emergency procedures can mitigate the risk of being locked-out (central instance managing access or zero-knowledge password proof in combination)

Table 36: Examination Details - Quality Attribute: Security & Privacy (II)

6 Results

A summary of the main findings identified during the ATAM is provided within the next chapter. All sensitivities, risks, non-risks and trade-offs observed are represented and described to understand the output of the architectural evaluation.

6.1 Sensitivities Identified

The sensitivity analysis revealed overall 19 sensitivities occurring 30 times within the proposed architecture. As reflected in figure 17, most sensitivities have been identified for AD3 (monitoring module), AD7 (transaction monitoring) and AD2 (extract module) raising concerns towards the communication, security & privacy and performance quality attributes. Least sensitivities have been identified for AD6 (limited attributed visibility), AD8 (patient summary archetype) and AD1 (openEHR archetypes) within the areas of evolution and communication.

The most frequent sensitivity point is *C-S2a* occurring five times raising general concerns over the message load the system is confronted with. This sensitivity point impacts the extract and monitoring module within the areas of communication, performance and medico-legal matters.

The second most frequent sensitivity points are *C-S1a* & *C-S5a* occurring both three times. *C-S1a* has an impact on AD1 (openEHR archetypes) raising concerns towards the communication, evolution- and medico-legal quality attributes in case the support for the openEHR reference model is discontinued. *C-S5a* raises concerns towards AD5 (role-based-access control system) and the complexity to create and maintain appropriate user access permissions impacting the communication, medico-legal and security & privacy quality attribute.

Table 38 summarises the occurrence of the identified sensitivities.

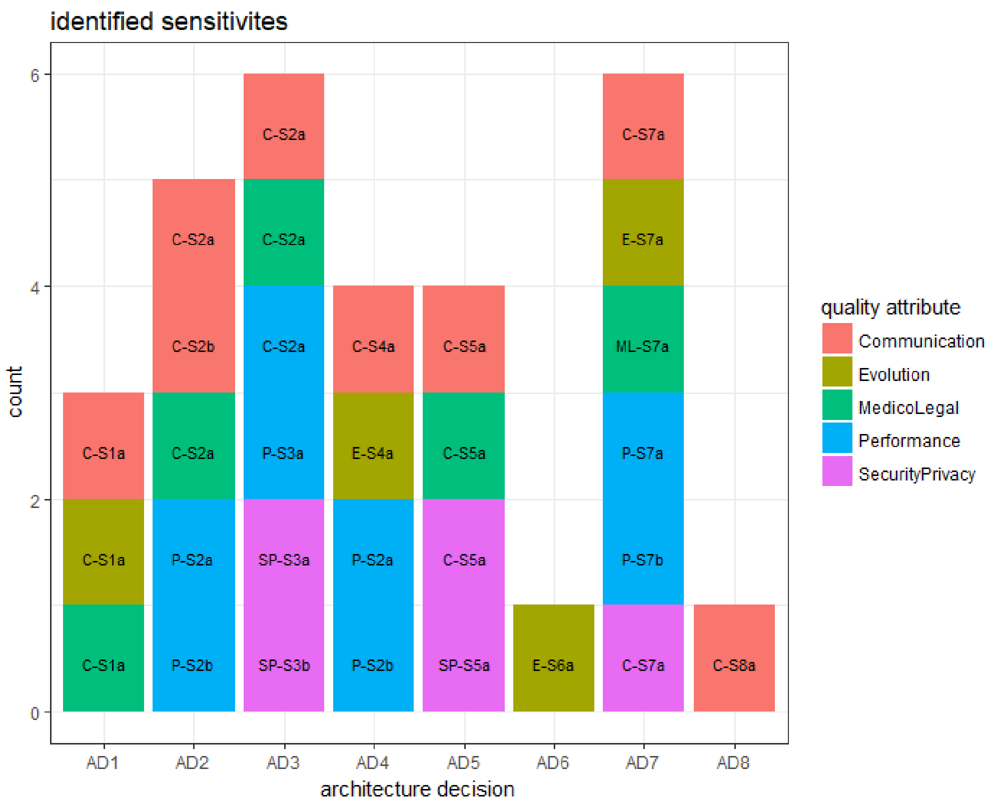


Figure 17: ATAM - Sensitivities

#	AD.ref	count
1	C-S1a	3
2	C-S2a	5
3	C-S2b	1
4	C-S4a	1
5	C-S5a	3
6	C-S7a	2
7	C-S8a	1
8	E-S4a	1
9	E-S6a	1
10	E-S7a	1
11	ML-S7a	1
12	P-S2a	2
13	P-S2b	2
14	P-S3a	1
15	P-S7a	1
16	P-S7b	1
17	SP-S3a	1
18	SP-S3b	1
19	SP-S5a	1

Table 37: ATAM - Sensitivity Counts

6.2 Risks Identified

The risk analysis identified 18 risks occurring 27 times within the assessed software architecture. As indicated within figure 17, AD7 (transaction monitoring) bears 6 risks which is the highest number compared to the remaining ADs. The risks identified in AD7 refer to all quality attributes identified. AD2 (extract module), AD3 (monitoring module) and AD4 (role-based access control system) bear the second highest number of risks within the software architecture. Those are mainly related to the communication and performance quality attributes. The least number of risks identified refer to AD6 (limited attribute visibility) and AD8 (patient summary archetype) which correlates to the sensitivities identified earlier.

The most frequent risk identified is *C-R2b*, describing the potentially heavy workload on both, legacy and patient summary systems, with an occurrence of four impacting AD2, AD3 & AD4 for communication and medico-legal related matters. The second highest risks are C-R1a describing the chance of potential harm to the architecture due to dispensed openEHR support and *C-R5a* describing the complexity to create sufficiently user access roles which correlates with the sensitivities identified previously. Note that AD1 (openEHR archetypes) bears three times the risk of *C-R1a* impacting the communication, evolution and medico-legal quality attribute indicating the importance to assure continuity for the openEHR reference model life cycle.

Table 39 provides an overview of the risk frequencies.

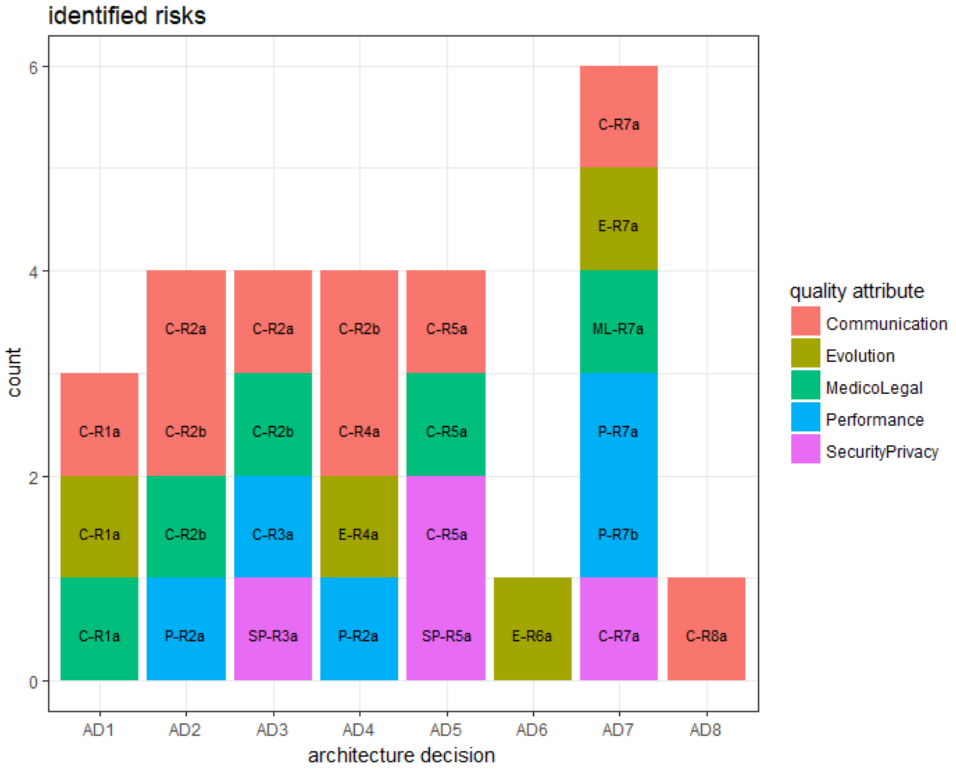
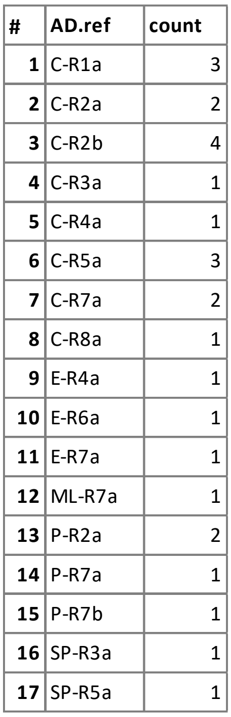


Figure 18: ATAM - Risks



#	AD.ref	count
1	C-R1a	3
2	C-R2a	2
3	C-R2b	4
4	C-R3a	1
5	C-R4a	1
6	C-R5a	3
7	C-R7a	2
8	C-R8a	1
9	E-R4a	1
10	E-R6a	1
11	E-R7a	1
12	ML-R7a	1
13	P-R2a	2
14	P-R7a	1
15	P-R7b	1
16	SP-R3a	1
17	SP-R5a	1

Table 38: ATAM - Risk Counts

6.3 Non-Risks Identified

Overall 21 non-risks have been identified in the software architecture occurring in total 33 times. As represented in figure 19, AD5 (role-based access control system) bears with a number of 9 most non-risks impacting the communication, evolution and medico-legal quality attribute. With a number of 8 bears AD1 the second most non-risks (openEHR archetypes) additionally affecting the security & privacy quality attribute. AD3 (monitoring module) contains the third most non-risks within the areas of communication, medico-legal, performance and security & privacy.

The biggest strength indicated by the ATAM is non-risk *C-N1a* with an occurrence of four describing the possibility to communicate among non- and openEHR compliant systems due to the openEHR reference model.

The second biggest strength of the architecture is related to the following three non-risks occurring three times each.

C-N1b: indicating the possibility to transfer created openEHR archetypes to other ontologies due to the two-levelling modelling approach impacting the communication, evolution and medico-legal quality attribute.

C-N5a: stating that the architecture is capable of dealing with highly granular user access permissions to assure that as much information as needed is granted to the user affecting the communication, medico-Legal and security & privacy quality attribute.

C-N5b: describing, that the architecture is able to avoid potential SoD violations based on the session-based design of the role-based access control system. This non-risk is impacting AD5 for the communication and security & privacy quality attribute and AD6 (limited attribute visibility) from the communication perspective.

Table 40 provides an overview regarding the non-risk frequency.

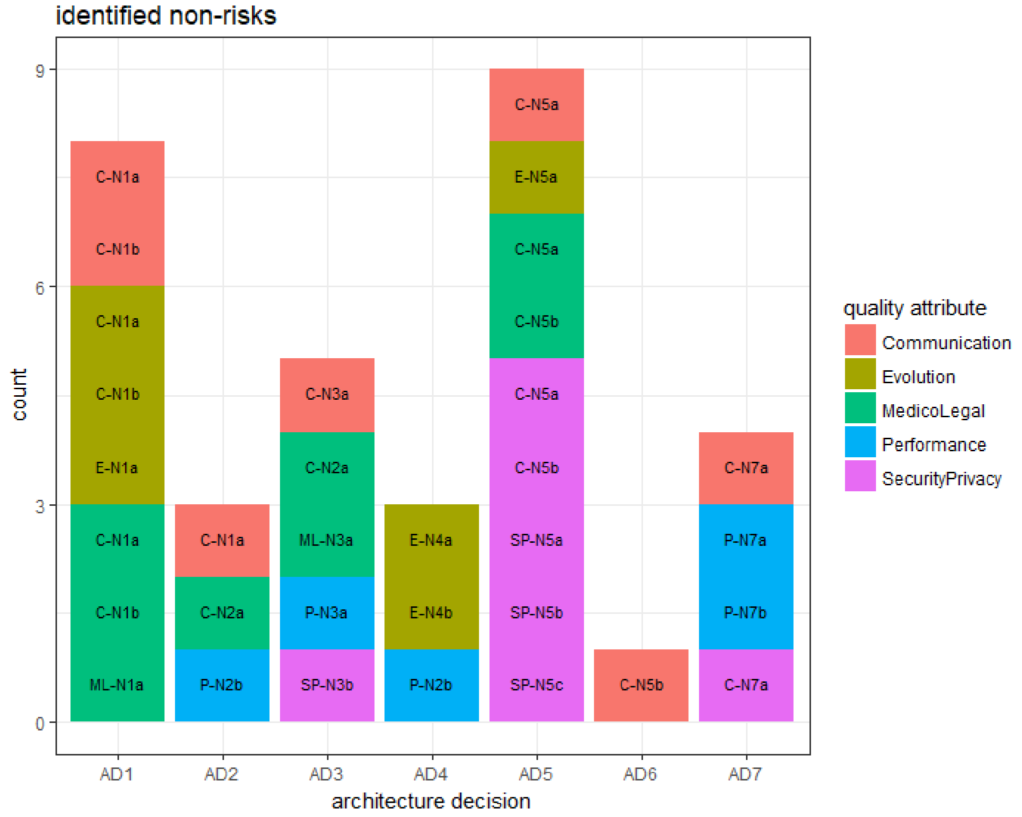


Figure 19: ATAM - Non-Risks

#	AD.ref	count
1	C-N1a	4
2	C-N1b	3
3	C-N2a	2
4	C-N3a	1
5	C-N5a	3
6	C-N5b	3
7	C-N7a	2
8	E-N1a	1
9	E-N4a	1
10	E-N4b	1
11	E-N5a	1
12	ML-N1a	1
13	ML-N3a	1
14	P-N2b	2
15	P-N3a	1
16	P-N7a	1
17	P-N7b	1
18	SP-N3b	1
19	SP-N5a	1
20	SP-N5b	1
21	SP-N5c	1

Table 39: ATAM - Non-Risk Counts

6.4 Trade-Offs Identified

To understand the software architectures fitness, trade-offs have been generated based on the identified sensitivities, risks and non-risks. Those are represented per AD and quality attribute within table 41 whereas a plus indicates a strength and a minus a weakness towards a quality attribute. As illustrated, the architecture contains most strengths towards the communication attribute assuring an exchange of a patient summary records from a variety of systems. This strength impacts mainly the performance and medico-legal quality attribute raising concerns towards the potential data load exposed to the system and concerns towards the violation of international regulations with a reference to Security & Privacy requirements. Another interesting trade-off has been identified regarding to the performance quality attribute. Depending if a permissioned or permission-less system is used for the architecture, security & privacy comes at the price of performance losses and the other way around. Permissioned environments are therefore considered as faster than permission-less environments are however considered as less secure. Regarding the evolutional quality attribute, the ATAM analysis revealed, that the architecture is capable of dealing with changes due to its modular architecture and by taking advantage of the openEHR reference model. A major weakness however arises, if the openEHR reference model is not being developed and updated further. From the medico-legal perspective, bears the architecture a strength for the cost of communication referring to authorisation questions.

Overall, the ATAM revealed strengths of the architecture to communicate among a variety of legacy systems and being compliant with well-known medical standards by making use of the openEHR reference model and the ISO18308 standard. This comes however with a major impact on performance related questions which is considered crucial for the end-user.

QA	AD#	Trade-Off	Communication	Security & Privacy	Performance	Evolution	Medico-Legal
Communication	AD1	C-T1a	+			-	+
	AD2	C-T2a	+		-		
	AD2	C-T2b	+				-
	AD4	C-T4a	+		-		-
	AD5	C-T5a	+	-			
	AD7	C-T7a	+	+	-		+
	AD8	C-T8a	+	-			-
Security & Privacy	AD3	SP-T3b		-			+
	AD5	SP-T5a	-	+			
Perfor-mance	AD2	P-T2b		+	-		+
	AD7	P-T7a		+	-		+
	AD7	P-T7b		-	+		
Evolution	AD4	E-T4a	-			+	
	AD6	E-T6a	-	+		-	
Medico-Legal	AD7	ML-T7a	-		-		+
Total +			7+	5+	1+	1+	6+
Total -			4-	4-	6-	2-	3-

Table 40: ATAM - Trade-Offs

7 Discussion

The objective of this chapter is to reflect on the results obtained throughout the research and discuss possible implications for being able to reach a conclusion. The following section discusses therefore the findings observed followed by the description of identified threats to validity.

7.1 Findings

The proposed software architecture described how interoperability issues within the medical field can be overcome. The key architectural decision for this was by making use of the openEHR reference model enabling semantical interoperability for medical data and simultaneously being compliant with common healthcare regulations. The big advantage by using the openEHR reference framework is, that healthcare providers do not need to change their technology backbone to participate in the system which is often related to high investments and potential changes in the medical process resulting into reluctance to innovate. One of the potential issues towards the reference model is, that openEHR is an association driven by its input of the community. Continuity can only be guaranteed when this input is assured over a steady period of time and is therefore crucial for the survival of the architecture. Given the fact, that the openEHR reference model has been deployed by a number of governments such as for the Australian Digital Health Agency, the ministry of health Brazil, the NHS of UK and the ministry of health & family welfare for the government of India is an indicator that the reference model can be deployed for demanding healthcare use-cases and justifies the decision to make use of the openEHR reference model.

Another aspect important to reflect on is the fact that the architecture has been developed based on the requirements provided by the ISO 18308. This leads to the advantage, that the architecture has a sound base since the standard has been developed with the involvement of globally-established experts allowing to get certified by regulators claiming that the architecture meets high quality standards.

Concerning the applicability of the Blockchain technology, the study revealed major concerns towards the implementation of a permission-less Blockchain due to the following three reasons:

1. The anonymity of nodes participating in the network potentially violates national and international laws in terms of data protection and information security.
2. The architectures continuity is at risk in respect to the network maintenance. Without having an ensured incentive to participate in the network stability such as for the described PoW environments based on mining, the architecture is prone to fail due to the mentioned tragedy of the commons theory. Current initiatives offer i.e. the possibility to hold stake based on tokens offered to the community entailing a value which is driven by financial incentives. In case the value drops, participants could leave the network since it becomes financially inefficient to participate bearing the risk of a network break-down.
3. The current PoW consensus mechanisms are able to cope with the described performance requirements, might however not be able to upscale in case of expansion of the use-case to other countries despite the Netherlands. By the time of this writing, several research and commercial initiatives are ongoing to solve this problem, potential solutions are however not yet provided.

Permissioned environments would provide remedy to those concerns. It would be therefore possible to be compliant with national and international laws, assurance of upwards scalability and network continuity for the price of semi centralising the environment. Contrary to expectations, the study revealed that a permissioned environment would offer a higher level of security to sustain a network and the possibility offer transparency to the patient concerning the access monitoring of their healthcare data.

A general concern identified within the study is towards user authorisation to Blockchains and how private keys can be managed and recovered since the loss of those would result into inaccessibility to the healthcare data. A solid mechanism capable of dealing with errors such as the key recovery, having emergency procedures applied would aid the general acceptance of the proposed architecture.

The most interesting finding revealed was related to the governance of the system preferably established by a public authority i.e. national government or European Union. Reasons being that governments are in charge to issue healthcare policies coordinating healthcare systems to meet health needs by the population. Due to demographic changes in our society, healthcare systems are facing massive challenges and need to be improved to meet future demands. Governments are therefore pressured and confronted to embrace disruptive changes, to increase transparency towards the population and improve efficiency. This would lead to a number of benefits such as a better unified access to healthcare data enabling a wide range of trend discoveries, i.e. for the case of vaccination status of a population and having the possibility to meet the demand when needed beforehand or providing anonymised data to support research projects. To spark further innovation in this field regulators have to consider, that established regulations generally reallocate financial resources away from innovation shifted towards regulatory compliance activities. The government is therefore in charge to maximise regulations that incentivise innovation within the field of healthcare IT instead of dis-incentivise.

7.2 Threats to Validity

The main threats concerning the validity and limitation of the research can be categorised into conclusion validity, construct validity and external validity. Given the fact, that only a limited number of five participants validated the architecture during the ATAM testing conclusion validity threats arise. A bigger number of participants could have widened the spectrum of prioritised scenarios the architecture shall deal with. Furthermore, there was only a limited amount of domain specialists involved dealing with electronic healthcare records providing their input.

A threat concerning the construct validity is regarding to the choice of quality attributes the architecture is based on. The SLR revealed the most important areas, however additional attributes within the area of i.e. availability or usability have not been considered and are not reflected within architecture.

Lastly, a threat towards the external validity arises due to the fact that the architecture has only been designed on a piece of paper without developing a prototype which could be assessed against the quality attributes in greater detail and identify gabs within the architectures design.

8 Conclusion

The previous chapters described the development of a software architecture to overcome EHR interoperability issues. Within the following chapter, the previously stated research questions are addressed to conclude on the overall research project.

The main research question was formulated as follows: "*How can the Blockchain technology overcome current EHR interoperability challenges?" and has been addressed by answering the following sub-research questions.*

SRQ1: *What are important stakeholder requirements for a Blockchain-based EHR architecture based on the current solutions available?*

The stakeholder requirements have been identified based on an SLR and are reflected thoroughly in chapter 3.2. The most important stakeholder requirements identified were towards Security & Privacy, Performance, Communication, Medico-Legal and Evolution which have been taken into account for the design of the software architecture. Those requirements are entailed in a variety of established standards within the area of transport, terminology, content and security & privacy. The ISO 18308 provides a set of requirements covering those areas justifying the decision to follow this specific standard for the design of the software architecture. The SLR also revealed three known types of EHR-Systems categorised as centralised infrastructure, de-centralised infrastructure and semi de-centralised infrastructure.

SRQ2: *What are current Blockchain technologies available, suitable for a Blockchain-based EHR?*

The SLR performed towards SRQ2 revealed that Blockchain technologies can be classified into the types of: permission-less, permissioned and hybrid systems described in detail in chapter 3.3. Taking the identified stakeholder requirements into account, it turned out, that permissioned systems would be most applicable for a Blockchain-based EHR due to scalability, security & privacy and medico-legal reasons reflected in chapter 7.1.

SRQ3: *How does a Blockchain-based EHR architecture look like taking all functional and technical stakeholder requirements into account?*

The architectures designed are represented in chapter 4 covering the context, functional, informational and partly development view of a software architecture. The main components identified are an *extract module* taking care of the data extraction process, a *mapping module* converting the obtained data to the openEHR reference module, a *role-based access management module* defining user and access permissions, a *monitoring module* assuring a holistic audit trial of the patient summary and a *smart contract module* interfacing with the Blockchain.

SRQ4: *What is the behaviour of a developed architecture taking important features (stakeholder requirements) into account?*

The behaviour of the proposed architecture has been assessed within chapter 5 and summarised in chapter 6. Based on the sensitivity points identified several risks and non-risks could be identified. As described within the result section, the architecture bears major risks towards a potentially heavy workload impacting the performance quality attribute. Furthermore, the ATAM revealed concerns towards the architecture life-cycle due to the dependency of the openEHR reference model and complexity concerns to create sufficient user access permissions.

The biggest strength identified is, that the architecture is capable to obtain patient data from any EHR without demanding a change in the current legacy landscape. Furthermore, is the architecture capable to define granular user access permissions with the possibility to avoid potential SoD violations.

SRQ5: *What are the identified trade-offs of the developed and tested architecture for a realistic implementation?*

The trade-off analysis is described in chapter 6 and revealed that the architecture is capable to communicate among a variety of EHR-Systems impacting the performance and medico-legal quality attribute. Furthermore, impacts the Security & Privacy quality attribute the Performance quality attribute. A balance between both quality attributes is needed to reach an acceptable level of transaction speed and latency as well as information security. Another trade-off has been identified concerning the medico-legal quality attribute impacting the communication quality attribute.

9 References

Acharya, D., & Kumar, V. (2010). A secure pervasive health care system using location dependent unicast key generation scheme. *Proceedings of the 3rd Workshop on Ph.D. Students in Information and Knowledge Management - PIKM '10*, 87. https://doi.org/10.1145/1871902.1871919

Adane, K., Muluye, D., & Abebe, M. (2013). Processing medical data: a systematic review. *Archives of Public Health*, *71*, 1. https://doi.org/10.1186/0778-7367-71-27

Al Jarullah, A., & El-Masri, S. (2012). Proposal of an architecture for the national integration of Electronic Health Records: A semi-centralized approach. *Studies in Health Technology and Informatics*, *180*, 917–921. https://doi.org/10.3233/978-1-61499-101-4-917

Austin, A., Smith, B., & Williams, L. (2010). Towards improved security criteria for certification of electronic health record systems. *Proceedings of the 2010 ICSE Workshop on Software Engineering in Health Care - SEHC '10*, 68–73. https://doi.org/10.1145/1809085.1809094

Barbacci, M. R., Carriere, S. J., Feiler, P. H., Kazman, R., Klein, M. H., Lipson, H. F., … Weinstock, C. B. (1998). Steps in an Architecture Tradeoff Analysis Method: Quality Attribute Models and Analysis. Retrieved from https://resources.sei.cmu.edu/asset_files/TechnicalReport/1998_005_001_16604.pdf

Barbacci, M. R., Ellison, R., Lattanze, A. J., Stafford, J. A., Weinstock, C. B., & Wood, W. G. (2003). Quality Attribute Workshops, Third Edition. *Quality*, (August), 38. https://doi.org/Technical Report CMU/SEI-2003-TR-016

Bartoletti, M., & Pompianu, L. (2017). An empirical analysis of smart contracts: platforms, applications, and design patterns, 1–16. Retrieved from http://arxiv.org/abs/1703.06322

Benson, T. (2005). Care Pathways, (August), 1–44. Retrieved from http://www.openclinical.org/docs/ext/briefingpapers/bensonPathways.pdf

Bentov, I., Lee, C., Mizrahi, A., & Rosenfeld, M. (2014). Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake. *Cryptology ePrint Archive*, *452*(3), 1–19. https://doi.org/10.1145/2695533.2695545

Bergmann, J., Bott, O. J., Pretschner, D. P., & Haux, R. (2007). An e-consent-based shared EHR system architecture for integrated healthcare networks. *International Journal of Medical Informatics*, *76*(2–3), 130–136. https://doi.org/10.1016/j.ijmedinf.2006.07.013

BinSubaih, A., & Maddock, S. (2006). Using ATAM to evaluate a game-based architecture. *… Architecture-Centric Evolution (ACE …*. Retrieved from http://staffwww.dcs.shef.ac.uk/people/S.Maddock/publications/BinSubaihMaddock2006_ACE.pdf

Brinkkemper, S., & Pachidi, S. (2010). Functional Architecture Modeling for the Software Product Industry. *Software Architecture SE - 16*, *6285*, 198–213. https://doi.org/10.1007/978-3-642-15114-9_16

Budgen, D., & Brereton, P. (2006). Performing systematic literature reviews in software engineering. *Proceeding of the 28th International Conference on Software Engineering - ICSE '06*, *2*, 1051. https://doi.org/10.1145/1134285.1134500

Buterin, V. (2014). Ethereum: A Next-Generation Cryptocurrency and Decentralized Application Platform. *Bitcoin Magazine*. Retrieved from https://bitcoinmagazine.com/ethereum-next-generation-cryptocurrency-decentralized-application-platform-1390528211%5Cnhttps://bitcoinmagazine.com/articles/ethereum-next-generation-cryptocurrency-decentralized-application-platform-1390528211

Commission, E. (2012). *eHealth Action Plan 2012-2020. Innovative healthcare for the 21st* *century*. https://doi.org/SWD(2013) 527

D'Amore, J. D., Mandel, J. C., Kreda, D. A., Swain, A., Koromia, G. A., Sundareswaran, S., … Ramoni, R. B. (2014). Are Meaningful Use Stage 2 certified EHRs ready for interoperability? Findings from the SMART C-CDA Collaborative. *Journal of the American Medical Informatics Association*, *21*(6), 1060–1068. https://doi.org/10.1136/amiajnl-2014-002883

Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., & Wang, F. (2017). Secure and Trustable Electronic Medical Records Sharing using Blockchain. *arXiv Preprint arXiv:1709.06528*.

eHealth Network. (2013). *Guidelines on Minimum / Non- Exhaustive Patient Summary Dataset for Electronic Exchange in Accordance With the Cross-Border Directive 2011 / 24 / Eu*. Retrieved from https://ec.europa.eu/health//sites/health/files/ehealth/docs/guidelines_patient_summary_en.pdf

eHealth Stakeholder Group. (2014). eHealth Stakeholder Group report Perspectives and Recommendations on Interoperability, (March), 1–35.

Ferraiolo, D. F., Kuhn, D. R., & Chandramouli, R. (2003). Role-Based Access Control. *Components*, *2002*(10), 338. https://doi.org/10.1016/S1361-3723(02)01211-3

Flores Zuniga, a E., Win, K. T., & Susilo, W. (2010). Functionalities of free and open electronic health record systems. *International Journal of Technology Assessment in Health Care*, *26*(4), 382–389. https://doi.org/10.1017/S0266462310001121 [doi] S0266462310001121 [pii]

Gardazi, S. U., & Shahid, A. A. (2017). Compliance-Driven Architecture for Healthcare Industry, *8*(5), 568–577.

Gartner. (2016). Hype Cycle for Emerging Technologies. Retrieved from https://www.gartner.com/newsroom/id/2575515

Gartner, I. (2017). Top Trends in the Gartner Hype Cycle for Emerging Technologies, 2017 - Smarter With Gartner. Retrieved from https://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/

Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016). On the Security and Performance of Proof of Work Blockchains. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS'16*, 3–16. https://doi.org/10.1145/2976749.2978341

Hardin, G. (1970). The Tragedy of the Commons. *Annals of Internal Medicine*.

Hevner, A. R. (2007). A Three Cycle View of Design Science Research. *Scandinavian Journal of Information Systems*, *19*(2), 87–92. https://doi.org/http://aisel.aisnet.org/sjis/vol19/iss2/4

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*(1), 75–105. https://doi.org/10.2307/25148625

International Organization For Standardization. (2005). Health informatics - Electronic health record - Definition, scope and context. *Definition of Electronic Health Record*, *ISO/TR 205*, 27. https://doi.org/ISO/TR 20514:2005(E)

Ivan, D. (2016). Moving Toward a Blockchain-based Method for the Secure Storage of Patient Records.

Kakavand, H., Kost De Sevres, N., & Chilton, B. (2017). The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2849251

Kalra, D. (2006). Electronic Health Record Standards. *IMIA Yearbook of Medical Informatics*, 136–144. https://doi.org/10.1016/j.soncn.2011.04.007

Kashfi, H., & Torgersson, O. (2009). A migration to an openEHR-based clinical application. *Studies in Health Technology and Informatics*, *150*, 152–156. https://doi.org/10.3233/978-1-60750-044-5-152

Kazman, R., Klein, M., & Clements, P. (2000). ATAM : Method for Architecture Evaluation. *Cmusei*, *4*(August), 83. https://doi.org/(CMU/SEI-2000-TR-004, ADA382629)

Kewell, E., Adams, R., & Parry, G. (2017). Blockchain for Good? *Strategic Change: Briefings in Entrepreneurial Finance*, *forthcomin*(5), 429–437. https://doi.org/10.1002/jsc.2143

Krawiec, R., Housman, D., White, M., Filipova, M., Quarre, F., Barr, D., … Tsai, L. (2016). Blockchain: Opportunities for Health Care.

Lee, A. (2013). *Health Care Pays: Summary of the general hospitals branch report 2013*. Retrieved from https://www.nvz-ziekenhuizen.nl/_library/12799/Health care pays - branch report 2013.pdf

Lee, A. (2015). How to write Performance Requirements with Example | 1202Performance. Retrieved April 13, 2018, from http://www.1202performance.com/atricles/how-to-write-performance-requirements-with-example/

Liang, X., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K., & Njilla, L. (2017). ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability. *Proceedings - 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, CCGRID 2017*, 468–477. https://doi.org/10.1109/CCGRID.2017.8

Liberati, A., Altman, D. G., Tetzlaff, J., Mulrow, C., Gøtzsche, P. C., Ioannidis, J. P. A., … Moher, D. (2009). The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: Explanation and elaboration. *PLoS Medicine*. https://doi.org/10.1371/journal.pmed.1000100

Lin, C. H., Fann, Y. C., & Liou, D. M. (2016). An exploratory study using an openEHR 2-level modeling approach to represent common data elements. *Journal of the American Medical Informatics Association*, *23*(5), 956–967. https://doi.org/10.1093/jamia/ocv137

Linn, L. A., & Koo, M. B. (2014). Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research, 1–10.

Luu, L., Narayanan, V., Zheng, C., Baweja, K., Gilbert, S., & Saxena, P. (2016). A Secure Sharding Protocol For Open Blockchains. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS'16*, 17–30. https://doi.org/10.1145/2976749.2978389

Maldonado, J. A., Moner, D., Bosca, D., Angulo, C., Marco, L., Reig, E., & Robles, M. (2011). Concept-based exchange of healthcare information: The LinkEHR approach. *Proceedings - 2011 1st IEEE International Conference on Healthcare Informatics, Imaging and Systems Biology, HISB 2011*, (May 2014), 150–157. https://doi.org/10.1109/HISB.2011.18

Manski, S. (2017). Building the blockchain world: Technological commonwealth or just more of the same? *Strategic Change*, *26*(5), 511–522. https://doi.org/10.1002/jsc.2151

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Elsevier*.

Markus, M. L., Majchrzak, A., & Gasser, L. (2002). A design theory for systems that support emergent knowledge processes. *Mis Quarterly*. https://doi.org/10.2307/4132330

Mashima, D., & Ahamad, M. (2012). Enhancing accountability of electronic health record usage via patient-centric monitoring. *Proceedings of the 2nd ACM SIGHIT International Health*

Informatics Symposium, 409–418. https://doi.org/10.1145/2110363.2110410

Mcconaghy, T., Marques, R., Müller, A., De Jonghe, D., Mcconaghy, T. T., Mcmullen, G., … Granzotto, A. (2016). BigchainDB: A Scalable Blockchain Database. Retrieved from https://www.bigchaindb.com/whitepaper/bigchaindb-whitepaper.pdf

Menachemi, N., & Collum, T. H. (2011). RMHP-12985-benefits-and-drawbacks-of-electronic-health-record-systems. https://doi.org/10.2147/RMHP.S12985

Millieu Ltd, & Time.Lex. (2014). Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services, (March), 34. Retrieved from http://ec.europa.eu/health//sites/health/files/ehealth/docs/laws_report_recommendations_en.pdf

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from www.cryptovest.co.uk

Nunamaker, J. F., Chen, M., & Purdin, T. D. M. (1990). Systems development in information systems research. *Journal of Management Information Systems*. https://doi.org/10.1109/HICSS.1990.205401

Pease, M., Shostak, R., & Lamport, A. L. (1980). Reaching Agreement in the Presence of Faults. *ACM International Conference Proceeding Series*. Retrieved from http://delivery.acm.org/10.1145/330000/322188/p228-pease.pdf?ip=145.107.122.94&id=322188&acc=ACTIVE SERVICE&key=0C390721DC3021FF.4AD871FF6AD78CEE.4D4702B0C3E38B35.4D4702B0C3E38B35&__acm__=1518007125_d47d1b083c38542b287b55b9b127b8c0

Petek, R. (2017). Understanding Blockchain Platform Architectures and Implementation Styles. *Gartner Research*, (March).

Peterson, K., Deeduvanu, R., Kanjamala, P., & Boles, K. (2016a). A Blockchain-Based Approach to Health Information Exchange Networks. *Mayo Clinic*, (1), 10. Retrieved from https://www.healthit.gov/sites/default/files/12-55-blockchain-based-approach-final.pdf

Peterson, K., Deeduvanu, R., Kanjamala, P., & Boles, K. (2016b). A Blockchain-Based Approach to Health Information Exchange Networks. *Mayo Clinic*.

Popov, S. (2017). The Tangle. Retrieved from https://iota.org/IOTA_Whitepaper.pdf

Prakash, R. (2016). Adoption of block-chain to enable the scalability and adoption of Accountable Care. *NIST Workshop on Blockchain & Healthcare*, (August).

Roehrs, A., André Da Costa, C., Da, R., & Righi, R. (2017). OmniPHR: A distributed architecture model to integrate personal health records. *Journal of Biomedical Informatics*, *71*, 70–81. https://doi.org/10.1016/j.jbi.2017.05.012

Sachdeva, S., & Bhalla, S. (2012). Semantic interoperability in standardized electronic health record databases. *Journal of Data and Information Quality*, *3*(1), 1–37. https://doi.org/10.1145/2166788.2166789

Santos, M. R., Bax, M. P., & Kalra, D. (2010). Building a logical EHR architecture based on ISO 13606 standard and semantic web technologies. *Studies in Health Technology and Informatics*, *160*(PART 1), 161–165. https://doi.org/10.3233/978-1-60750-588-4-161

Stead MD, W. W., Kelly, MD, B. J., & Kolodner MD, R. M. (2005). Achievable Steps Toward Building a National Health Information Infrastructure in the United States. *Journal of the American Medical Informatics Association*, *12*(2), 113–120. https://doi.org/10.1197/jamia.M1685.tients

Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution*. *Blockchain Revolution*. https://doi.org/10.1515/ngs-2017-0002

Tapuria, A., Kalra, D., & Kobayashi, S. (2013). Contribution of clinical archetypes, and the challenges, towards achieving semantic interoperability for EHRs. *Healthcare Informatics Research*, *19*(4), 286–292. https://doi.org/10.4258/hir.2013.19.4.286

Teodoro, D., Sundvall, E., João Junior, M., Ruch, P., & Miranda Freire, S. (2018). ORBDA: An openEHR benchmark dataset for performance assessment of electronic health record servers. *Plos One*, *13*(1), e0190028. https://doi.org/10.1371/journal.pone.0190028

Vukolić, M. (2017). Rethinking Permissioned Blockchains. *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts - BCC '17*, 3–7. https://doi.org/10.1145/3055518.3055526

Wang, L., Min, L., Wang, R., Lu, X., & Duan, H. (2015). Archetype relational mapping - a practical openEHR persistence solution. *BMC Medical Informatics and Decision Making*. https://doi.org/10.1186/s12911-015-0212-0

Wieringa, R. (2014). *Design Science Methodology for Information Systems and Software Engineering*. *Springer Berlin Heidelberg*. https://doi.org/10.1145/1810295.1810446

Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., Regnell, B., & Wesslén, A. (2012). *Experimentation in software engineering*. *Experimentation in Software Engineering* (Vol. 9783642290). https://doi.org/10.1007/978-3-642-29044-2

Woods, E., & Rozanski, N. (2012). *SOFTWARE SYSTEMS ARCHITECTURE SECOND EDITION*. Retrieved from http://ptgmedia.pearsoncmg.com/images/9780321718334/samplepages/032171833X.pdf

Xu, X., Pautasso, C., Zhu, L., Gramoli, V., Ponomarev, A., Tran, A. B., & Chen, S. (2016). The blockchain as a software connector. *Proceedings - 2016 13th Working IEEE/IFIP Conference on Software Architecture, WICSA 2016*, (August), 182–191. https://doi.org/10.1109/WICSA.2016.21

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where Is Current Research on Blockchain Technology?-A Systematic Review. *PloS One*, *11*(10), e0163477. https://doi.org/10.1371/journal.pone.0163477

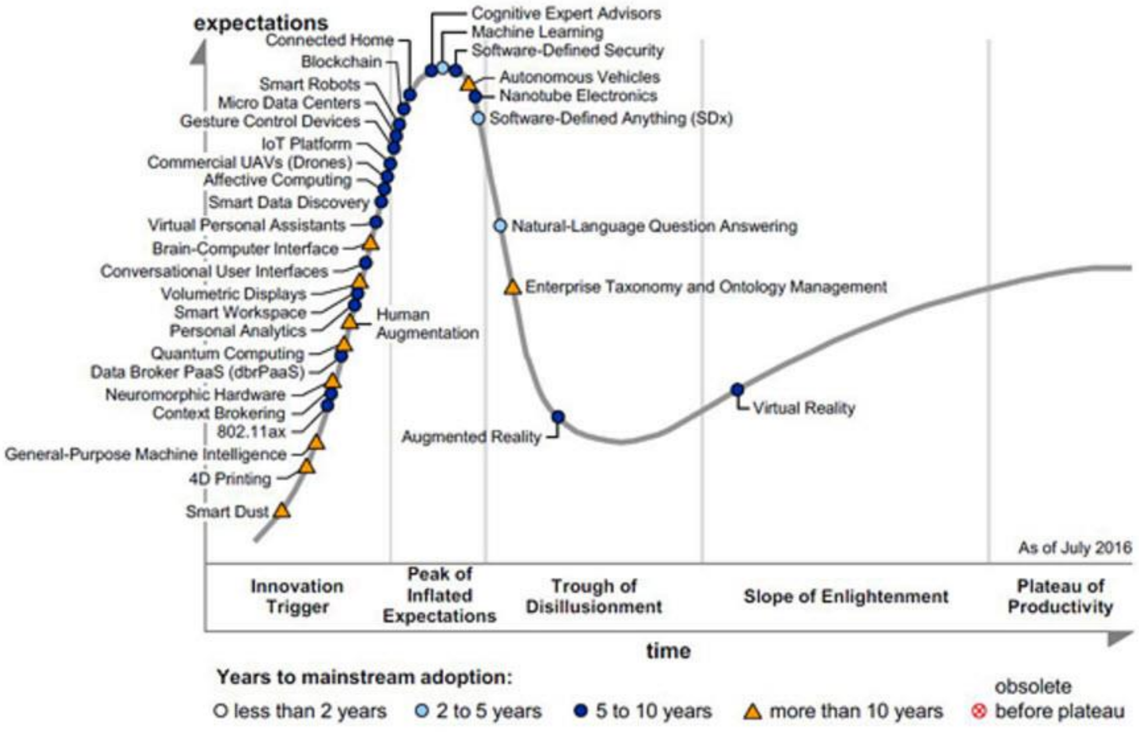
Zhang, P. (2015). Design of Blockchain-Based Apps Using Familiar Software Patterns to Address Interoperability Challenges in Healthcare.

10 Appendices

Table of content – Appendices

1. Appendix A: Gartner Hypecycle – Emerging Technologies, 2016

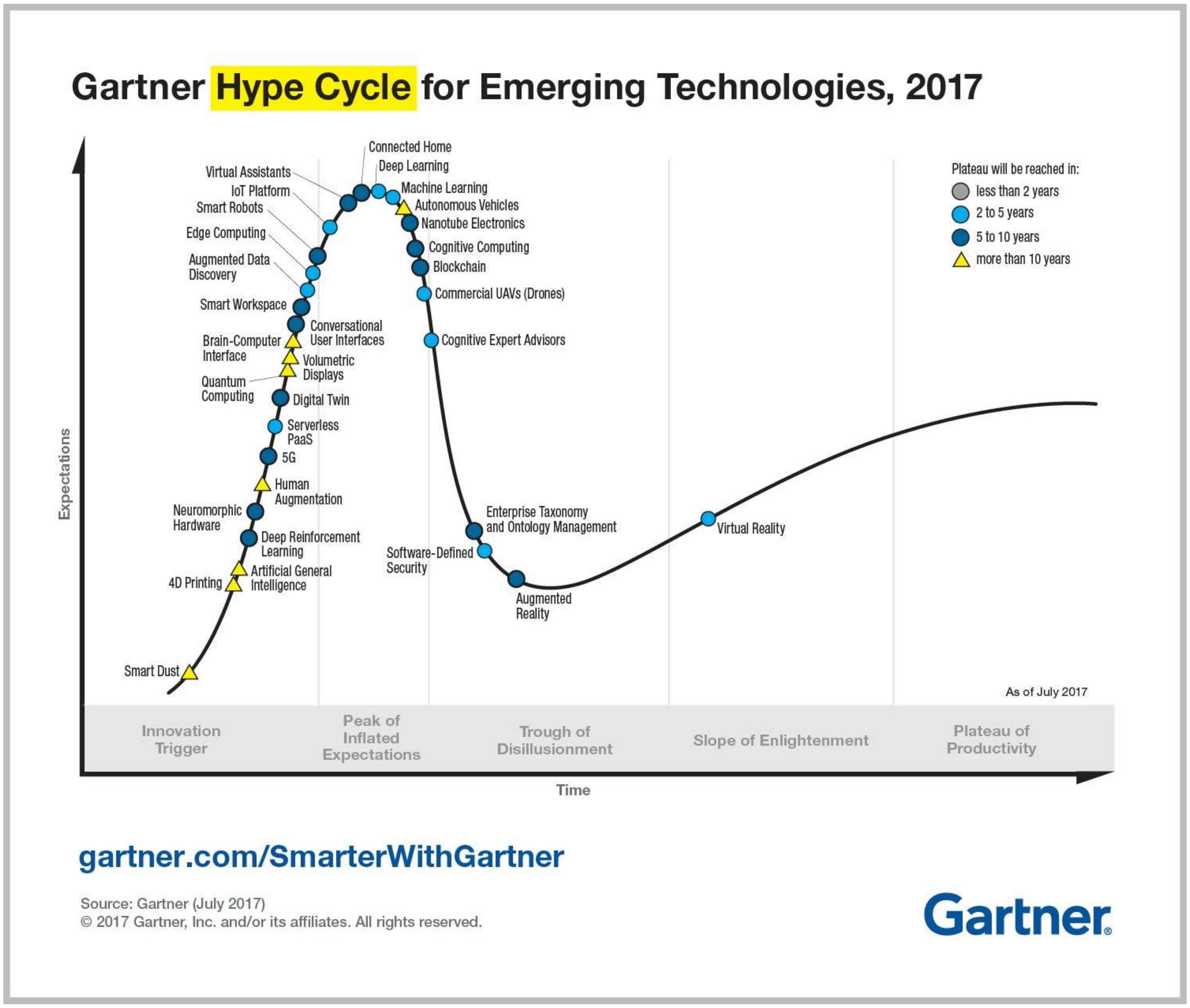
Figure 1. Hype Cycle for Emerging Technologies, 2016



Source: Gartner (July 2016)

Source: Gartner (August 2016)

2. Appendix B: Gartner Hype Cycle – Emerging Technologies, 2017


Gartner Hype Cycle for Emerging Technologies, 2017

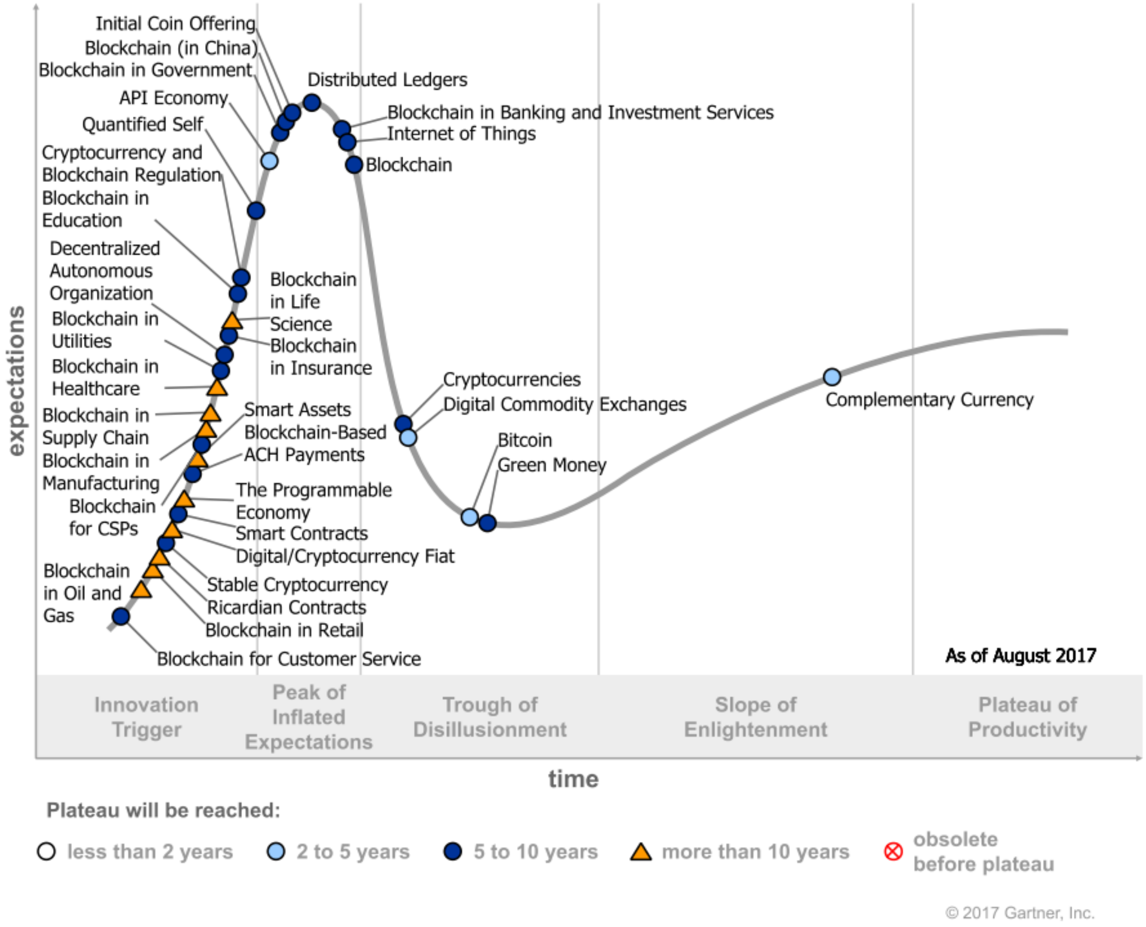
gartner.com/SmarterWithGartner

Source: Gartner (July 2017)

Gartner.

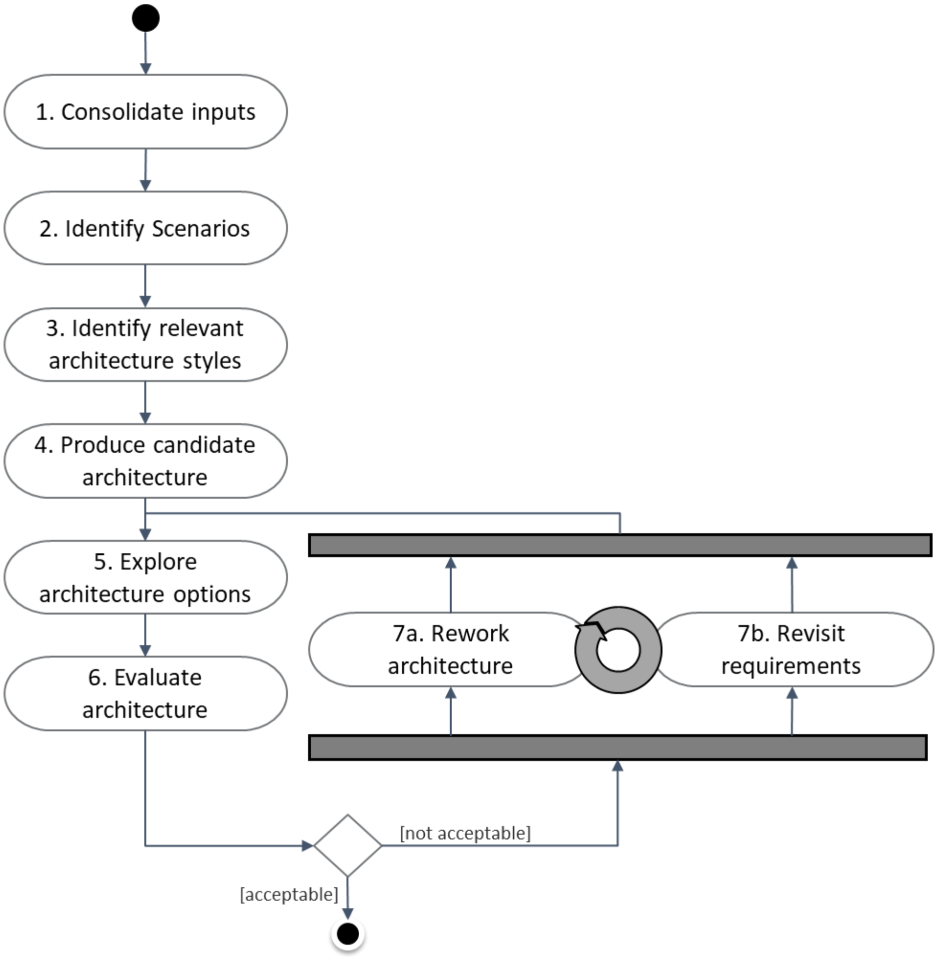
3. Appendix C: Gartner Hype Cycle – Blockchain Business, 2017

Figure 1. Hype Cycle for Blockchain Business, 2017



Source: Gartner (August 2017)

4. Appendix D – Architecture Definition Process



Architecture Definition Process (own creation in reference to Rozanski (2011))

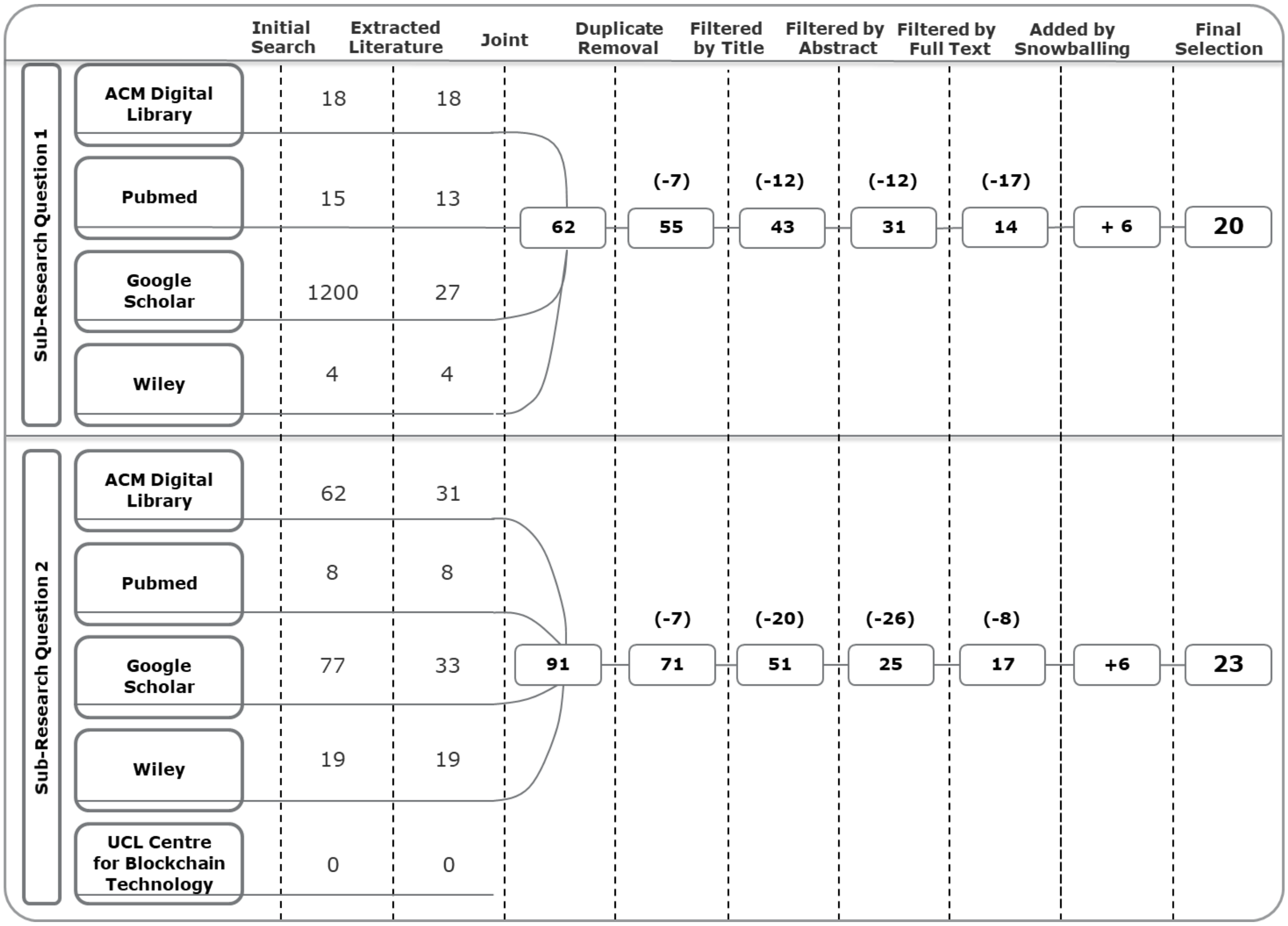
5. Appendix E: SLR – Search Results Overview

#	search engine	Query	# results	# Extracted
Sub-research question 1				
1	Pubmed	((((EHR[TW] OR PHR[TW] OR "electronic healthcare record"[TW] OR "electronic medical record"[TW])) AND (architecture[TW] OR "system design"[TW])) AND (regulation[TW] OR compliance[TW] OR requirement*[TW] OR "data standard"[TW])) AND ("2010/01/01"[Date - Publication] : "3000"[Date - Publication])	15	13
2	Wiley	EHR AND ARCHITECTURE	4	4
3	ACM	keywords.author.keyword:(EHR) AND recordAbstract:(architecture requirements)	18	18
4	Google Scholar	(EHR OR PHR OR "electronic medical healthcare records") AND (architecture OR "system design") AND (requirements OR "data standard")	12000	27
Sub-research question 2				
1	Pubmed	blockchain[OT]	8	8
2	Wiley	blockchain[abstract] AND 2010 - 2017	19	19
3	ACM	keywords.author.keyword:(blockchain)	62	31
4	Google Scholar	(Blockchain) AND (EHR OR PHR OR "electronic healthcare record" OR "personal healthcare record") filtered on everything	77	33
5	UCL Centre for Blockchain Technologies	The website did not allow querying; hence a manual search approach was applied. No relevant literature could be identified.	0	0

6. Appendix F: PRISMA Structured Summary Template:

#	Item	Notes
##	APA citation	
0	META (place, publication date, other demographic data	
1	Background	
2	Objectives	
3	Data sources	
4	Study eligibility criteria	
5	Participants and interventions	
6	Study appraisal and synthesis models	
7	results	
8	limitations	
9	Conclusions and implications of key findings	
10	Systematic review registration number	

7. Appendix G: SLR - Systematic Mapping



8. Appendix H: Healthcare Data Standards

#	Standard	Name	Category
1	ASC X12N	Accredited Standards Committee X12	Content, Transport
2	C-CDA	Consolidated CDA	Content
3	CCR	Continuity of Care Record	Transport
4	CDC CVX	Centers for Disease Control and Prevention	Terminology
5	CEN/TC 251	CEN Technical Committee 251	Terminology, Transport
6	CPT	Current Procedural Terminology	Terminology
7	DICOM	Digital Imaging and Communications in Medicine	Transport
8	Direct	Direct Project	Transport
9	FHIR	Fast Healthcare Interoperability Resources	Transport
10	HIPAA	Health Insurance Portability and Accountability Act	Privacy & Security
11	HITECH	Health Information Technology for Economic and Clinical Health Act	Terminology, Content
12	HITSP	Healthcare Information Technology Standards Panel	Terminology, Transport
13	HL7	Health Level-7	Content, Transport
14	ICD 10	International Statistical Classification of Diseases and Related Health Problems	Terminology
15	ICPC	International Classification of Primary Care	Terminology, Content
16	IHE	Integrating the Healthcare Enterprise	Transport
17	LOINC	Logical Observation Identifiers Names and Codes	Terminology
18	MEDCIN	System of standardized medical terminology	Terminology
19	NDC	National Drug Code	Terminology
21	RxNorm	RxNorm	Terminology
22	SNOMED CT	Systematized Nomenclature of Medicine--Clinical Terms	Terminology
23	UCUM	Unified Code for Units of Measure	Terminology
24	UMLS	Unified Medical Language System	Terminology, Content
26	xDT	German data exchange format	Transport

9. Appendix I: ISO/TR 18308:2004 Requirements

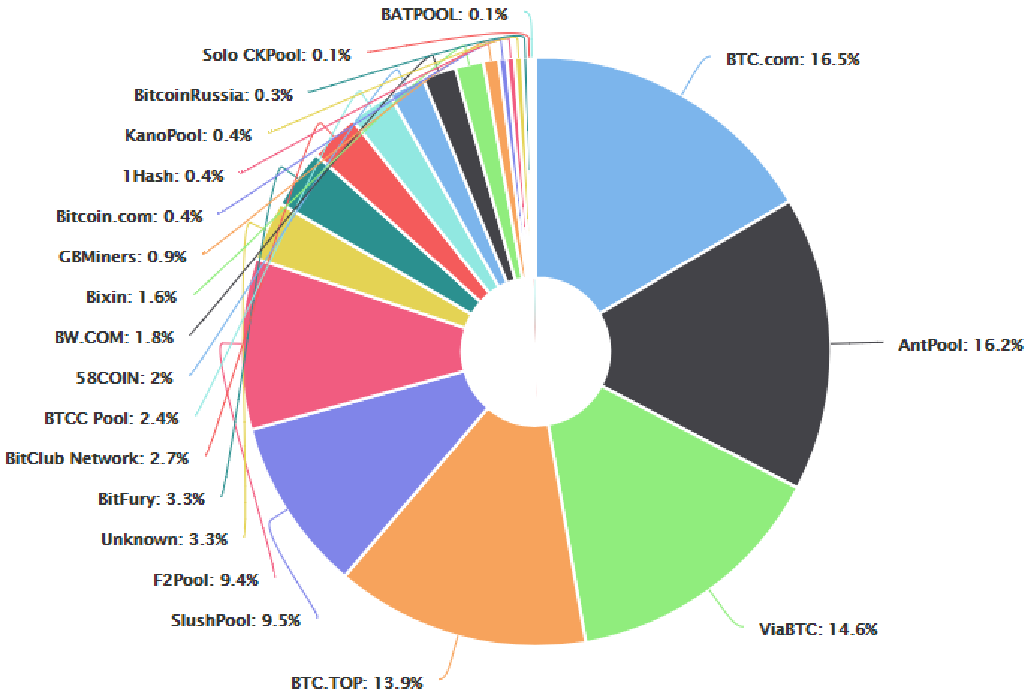
Section	Sub-Section	Requirement	Description
Structure			
	Record Organisation		
		Sections	The EHR must enable information in the EHR to be organised in different sections allowing navigation by users and views of sections to be returned as the result of queries.
		EHR Format	The EHR must ensure that the 'format' of the EHR as it appears to the clinician or user is able to conform to specifications set by standards organisations, regulatory and accreditation agencies, professional groups, local healthcare institutions and users.
		Portability	The EHR must support an EHR which is moveable and mergeable between individuals and institutions independent of hardware, software (application programs, operating systems, programming languages), databases, networks, coding systems, and natural languages.
		Secondary use	The EHRRA must enable information in the EHR to be organised and retrieved in a manner that facilitates its secondary uses.
		Archiving	The EHR must support archiving.
	Data Organisation	Structured Data	The EHR must enable storage of data as lists such that the order of the data is preserved when the data is displayed.
			The EHR must enable storage of data in tables such that the relationships of the data with the row and column headings are preserved.
			The EHR must enable storage of data in hierarchies such that the relationship between the node parents and children are preserved.
			The EHR must enable storage of data such that simple name/value pairing is preserved.
			The EHR must enable the storage of multiple values of the same measurement taken at closely proximate times at the same contact, or at different contacts and at different locations. The context of these measurements must be preserved - such as who took the measurement, what method was used etc. These values should be able to be returned in a query and ordered in different ways
		Non-Structured Data	The EHR must support the inclusion of narrative free text and there should be no logical limit to the size of this text.
			The EHR must support searching within non-structured data (text and non-text) and the inclusion of structured text within this data.
			The EHR must support the inclusion of comments within the data stored - enabling the clinician to qualify structured information appropriately. Comments must be able to be linked to specific data attributes.
			The EHR must provide a means for different levels of emphasis to be associated with comments and other entries - this may alter the way they are displayed or their returning in a query
		Clinical Data	The EHRRA must allow for comprehensive information storage and retrieval regarding patient care. The EHRRA must at a minimum allow for the recording of all data on: • Patient history • Physical examination • Psychological, social, environmental, family, and self care information • Allergies and other therapeutic precautions • Preventative and wellness measures such as vaccinations and lifestyle interventions • Diagnostic tests and therapeutic interventions such as medications and procedures • Clinical observations, interpretations, decisions, and clinical reasoning • Requests/orders for further investigation, treatments, or discharge • Problems, diagnoses, issues, conditions, preferences and expectations • Healthcare plans, health and functional status, and health summaries • Disclosures and consents • Suppliers, model and manufacturer of devices (e.g. implants or prostheses)
		Administrative Data	The EHR must support the recording (and classifying for identification purposes) of patient identification, location, demographic, contact, employment and other administrative data.
			The EHR must support standards for information which enable the unambiguous identification of the subject of care, the clinicians involved in care (including their role and context of care), the location of care, the date/time and duration of care, and third parties such as next of kin and non-clinical contacts. There should be no limit on the storage of such information.
			The EHR must support the administration of healthcare processes and episodes of care as well as the organisation of visit and encounter data.
			The EHR must support the recording of financial and other commercial information such as health plan enrolment, eligibility and coverage information, guarantor, costs, charges, and utilisation.
			The EHR must support the recording of legal status and consents relevant to the patient's healthcare (e.g. legal status of guardianship order, consents for operations and other procedures).
			The EHR must be amenable to querying for the purpose of data aggregation to support information gathering required for population and public health initiatives, surveillance, and reporting.
	Type and form of data	support different types of data	The EHR must allow for the incorporation of data types defined elsewhere, such as DICOM, MIME, EKG.
		Data types	Numeric and Quantifiable data. The EHR must support the definition of the logical structure of numeric and quantifiable data, including the handling of units.
			Quantities should include a measure of precision related to the method of measurement.
			Percentages must be able to be expressed as quantities.
			Quantity ranges The EHR must support the definition of the logical structure of ranges - that is high and low values.
			Quantity ratios The EHR must support the definition of the logical structure of quantity ratios (i.e. x of a per y of b)
			Dates and times The EHR must support the definition of the logical structure of dates and times.
			The EHR must support approximate, partial, and fuzzy dates and times such as: • approximate dates/times: e.g., sometime yesterday, last week; • partial dates: e.g. ??/May/1997, ??/??/1928

Section	Sub-Section	Requirement	Description
			The EHR must support the recording of future planned events or actions such as: • periods of day or time: e.g., morning, afternoon, evening, shifts (AM, PM, NOC), while awake; • points of time: e.g., upon awakening, at mealtime (breakfast, lunch, dinner), at bedtime; • relative points of day or time: e.g., before breakfast, after lunch, before bedtime, two days post discharge, one week after last dose; • alternating and patterned dates/times: e.g., alternate every 8 hours, alternate every 3 days, every Monday/Wednesday/Friday, every Sunday, every third Tuesday
			The EHR must support the recording of time as an absolute time, an elapsed time since a particular event, and as a duration.
			The EHR must support the recording of the time-zone in which the recording took place.
			The EHR must support recording of time in all units down to milliseconds.
		Reference Data	The EHR must support the recording of references such as normal ranges and attributes relevant to a particular observation or measurement
		Contextual Data	The EHR must support the recording of contextual data associated with the date/time the event occurred.
			The EHR must support the recording of contextual data associated with the date/time the event was committed to the record.
			The EHR must support the recording of contextual data associated with the subject.
			The EHR must support the recording of contextual data associated with the person responsible for recording and committing the event.
			The EHR must support the recording of contextual data associated with the healthcare facility.
			The EHR must support the recording of contextual data associated with the location where the event was recorded.
			The EHR must support the recording of contextual data associated with the reason for recording the information associated with the event.
			The EHR must support the recording of contextual data associated with the protocol associated with the event.
		Links	The EHR must define the semantic representation of links between different information in the EHR.
			The EHR must support links to 'externally referenced data' which is not able to be stored within the EHR, providing patient safety is not compromised.
	Supporting health concept representation	support for multiple coding systems	The EHR must support multiple coding systems (entry or interface terminologies, reference terminologies and classifications) by creating interfaces with electronic tools such as terminology browsers, terminology editors and terminology servers.
			At the data attribute level, the EHRRA must support the capture of the code, the coding scheme (e.g., coding/classification system), version and original language.
			The EHRRA must enable storage of data from terminologies and preserve the information about the terminology set from which it was chosen.
		Unique representation of information	Where information is not represented uniquely in only one place and one way, the EHR shall support explicit rules to avoid ambiguity (e.g. is must be clear what [not] [pedal pulses absent] means).
			The EHR must support a means of mapping between objects in information and inference models corresponding to a well-defined set of concepts in the foundation reference terminology (or concept) model.
		Language independence	The EHRRA must support the use of a comprehensive reference terminology that enables the recording/translation of multilingual terms. [This does not imply that a given EHR implementation must support more than one language].
			The EHRRA must support the identification of information that has been translated from the language in which it was originally recorded. Such identification must describe the faithfulness or reliability of the translation.
		Representation of text	The original textual representation as entered by the clinician must be retained in the EHR when information is translated from one natural language to another or when terms are mapped from one coding/classification system to another.
Process	Clinical Process	Support for clinical processes	The EHR must support the recording of any type of clinical event, encounter, or episode relevant to the care of a patient.
			The EHR must support the creation, instantiation, and maintenance of clinical processes that support the activities of its users.
			The EHR must support the continuity of a clinical process, the ability to query the status of a process, modify an existing process, and verify that a process has been completed.
			The EHR must be able to accommodate partial completion of a clinical process.
		Problems/issues and health status	The EHR must support the recording and presentation of holistic health status, functional status, problems, conditions, environmental circumstances and issues.
			The EHR must support the recording and presentation of data in a problem-oriented structure including problem status, resolution plans and targets (problem-oriented here includes conditions and issues).
			The EHR must support a patient's lifetime, longitudinal record of health status and care interventions which can be viewed as a chronological health record. The patient EHR is at once (simultaneously): 1. retrospective: an historical view of health status and interventions (e.g., completed health service events/acts); 2. concurrent: a "now" view of health status and active interventions (e.g., health service events/acts now underway); and 3. prospective: a future view of planned interventions (e.g., health service events/acts scheduled or pending).
		Clinical reasoning	The EHR must support the recording of the clinical reasoning including automated processes for all diagnoses, conclusions, and actions regarding the care of a patient.
		Decision support, guidelines, and protocols	The EHR must support the automatic presentation of warnings, alerts and reminders such as patient infective status, allergies and other therapeutic precautions, outstanding interventions, and urgent results.
			The EHR must support systematic population-based recalls and reminders including public and population health programs such as immunisation and epidemiological surveillance.
			The EHR must be able to support guidelines, protocols, and decision support systems.
			The EHR must enable semantic interoperability of clinical concepts to support decision support processing.
		Care planning	The EHR must support care planning, including the management of process states (e.g. planned, ordered, scheduled, in progress, on hold, pending, completed, amended, verified, cancelled), within the care planning process.
		Orders & service processes	The EHR must support the recording and tracking of clinical orders and requests such as prescriptions and other treatment orders, investigation requests, and referrals.
			The EHR must support the linking of orders with the observations that arise as a result (e.g. the results of an investigation or administration of a medication with the order for these interventions).
		Integrated care	The EHR must support integrated patient care including continuing collaborative multi-disciplinary care and case management across different healthcare sectors and settings (e.g. primary care, acute hospitals, allied health, home-based care).
		Quality assurance	The EHR must support the recording and querying of data to enable the measurement of operational and clinical performance, to ensure compliance with standards of care, to ensure quality process and to measure outcomes.

Section	Sub-Section	Requirement	Description
	Record processes		
		Data capture	The EHR must support clear and consistent rules for entry, amendment, verification, transmittal, receipt, translation, and deletion of data. This requirement does not imply that it is necessary for a given implementation to allow deletion of EHR content. Local data retention rules will apply
			The EHR must support the implementation of rules for data validation.
			The EHR must support the ability to review information of all types recorded in the past, including via the use of query and filter facilities, during the data capture process
		Retrieval/query/views of data	The EHR must support selective retrieval and customized views of the same information for specific needs (e.g. decision support, data analysis).
		Presentation of data	The EHR must support the ability to display data marked as clinical summary without the need for manual searching.
			The EHR must support the ability to convey the nature of devices on which information should by preference be presented where this may affect the clinical interpretation (e.g. viewing a colour image on a monochrome viewer, viewing a digital diagnostic image on a low resolution viewer).
		Scalability	The EHR should not impede efficient processing of very large records or very large numbers of records.
Communication			
	Messaging		The EHR must support the export and import of data received using messaging protocols such as HL7, UN/EDIFACT and DICOM.
	Record exchange		The EHR must allow for the exchange of a complete EHR or a part of an EHR (an extract) between EHRRA compliant systems.
			The EHR must support serialisation of data for interoperability purposes (e.g. via XML, CORBA, SOAP, etc.).
			The EHR must define the semantics of merging data from an EHR extract with the EHR resident in the receiving system.
			The EHR must provide an audit trail of exchange processes, including authentication, to enable identification of points of EHR extract transmittal and receipt. This needs to account for merging processes.
			The rules covering the exchange of an extract must be the same as those for exchanging the complete record.
			The EHR must enable semantic interoperability of clinical concepts between EHR systems to support automatic processing of data at the receiving system.
Privacy & Security			
	Privacy and confidentiality		The EHR must support the application of prevailing privacy and confidentiality rules.
			The EHR must support the labelling of the whole and/or sections of the EHR as restricted to authorised users and/or purposes. This should include restrictions at the level of reading, writing, amendment, verification, and transmission/disclosure of data and records
			The EHR must support privacy and confidentiality restrictions at the level of both data sets and discrete data attributes.
	Consent		The EHR must support recording of informed consent for the creation of a record.
			The EHR must support obtaining, recording and tracking the status of informed consent to access the whole and/or sections of the EHR, for defined purposes.
			The EHR must support recording of the purposes for which consent is obtained.
			The EHR must support recording of the time frames attached to each consent.
	Access control		The EHR must support measures to define, attach, modify and remove access rights to the whole and/or sections of the EHR.
			The EHR must support measures to define, attach, modify and remove access rights for classes of users of the EHR.
			The EHR must support measures to enable and restrict access to the whole and/or sections of the EHR in accordance with prevailing consent and access rules.
			The EHR must support measures to separately control authorities to add to and/or modify the EHR from authorities to access the EHR
	Data integrity		The EHR must support measures to ensure the integrity of data stored in and transferred to and from EHRs
	Auditabilty of access		The EHR must support recording of an audit trail of access to and modifications of data within the whole or sections of the EHR.
			The EHR must support recording of the nature of each access and/or transaction.
			The EHR must support audit capability sufficient to track accountability for each step or task in the clinical or operational processes recorded in the record.
Medico-Legal			
	Support for legal requirements		The EHR must support measures to ensure an accurate reflection of the chronology of clinical events and information availability in the EHR.
			The EHR must enable the viewing of an accurate representation of the EHR at any particular date and time since its creation.
	Actors		
		Subject of healthcare	The EHR must cater for the subject of care of the EHR to be one or more persons
		Patient identification	The EHR must cater for the recording of appropriate patient identification attributes and clinically relevant patient attributes such as date of birth, sex, ethnicity etc.
		User Identification	The EHR must ensure that users who attest and commit any particular information to the record are uniquely and reliably identified.
			The EHR must support the on-going ability to identify users, even if they change their name, profession, sex, or address.
		Healthcare parties	The EHR must support measures to ensure that all clinical parties referred to in the HER are uniquely identified.
			The EHR must support the recording of the clinical roles of any parties with respect to any clinical activity recorded.
		Author responsibility	The EHR must support measures which ensure that every record entry is dated, its author identified.
			The EHR must support measures to ensure that there is an absolute requirement that each contribution to the record is attributed to a responsible healthcare party whether in the role of author or not.
		Attestation/Authorisation of entries	The EHR must support measures which ensure that every contribution to the record must be attested by a responsible person.
			The EHR must support measures which ensure that amendments are attributed to a responsible person and the date and time and the reason for the amendment are recorded.
	Clinical competence/governance		The EHR must support the demonstration of clinical competence and accountability of clinicians.
	Faithfulness		The EHR must ensure that information intended to supersede that already recorded and attested must be separately collected and attested as a new transaction version.
			The EHR must ensure that the exact state of the record can be re-created for any given point of time since the original creation of the EHR.
	Preservation of context		Where coded terms in the EHR have been mapped to another coded terminology, the EHR must provide a means of indicating the faithfulness of the translation
			The EHR must maintain the original context of all elements of the record irrespective of the potential separate distribution of elements.
	Permanence		The EHRRA must ensure that attested information shall be stored in a protected mode, disallowing any changes or deletions.
			The EHR will ensure that amendments are attributed to a clinician and the date and time, and the reason for the amendment are recorded.
	Version control		The EHR must incorporate a method of version control that supports information at the level at which it was attested
			The EHR must support measures to discern modification or updating of the record using version control.

Section	Sub-Section	Requirement	Description
Ethical	Support for ethical justification		The EHR must be able to record ethical approval for secondary uses of patient information held in the EHR.
Consumer/Cultural	Consumer issues	Support for consumer issues	The EHRRA must support the production of a consumer oriented view.
			The EHR must support consumers' right of access to all EHR information subject to jurisdictional constraints.
			The EHR must support consumers being able to incorporate self-care information, their point of view on personal healthcare issues, levels of satisfaction, expectations and comments they wish to record in EHRs.
	Cultural issues	Support for cultural issues	The EHR must support interoperability in a way that is truly global, yet respects local customs and culture. It follows that the process must be both simple and amenable to customisation in different jurisdictions.
Evolution	Support for EHR architecture and EHR system evolution		Backwards compatibility of EHR software: Any implementation of the EHR must be able to process EHRs created under older versions of the HER.
			Backwards compatibility of the EHR: Software built on a previous version of the EHR must be capable of processing EHRs created under a newer version of the EHR.
			The EHR must be able to accommodate the recording of information due to new forms of clinical knowledge, new clinical disciplines, and new clinical practices and processes.

10 Appendix J: Bitcoin Mining Pool Distribution



Obtained from: https://blockchain.info/pools on 05.12.2017

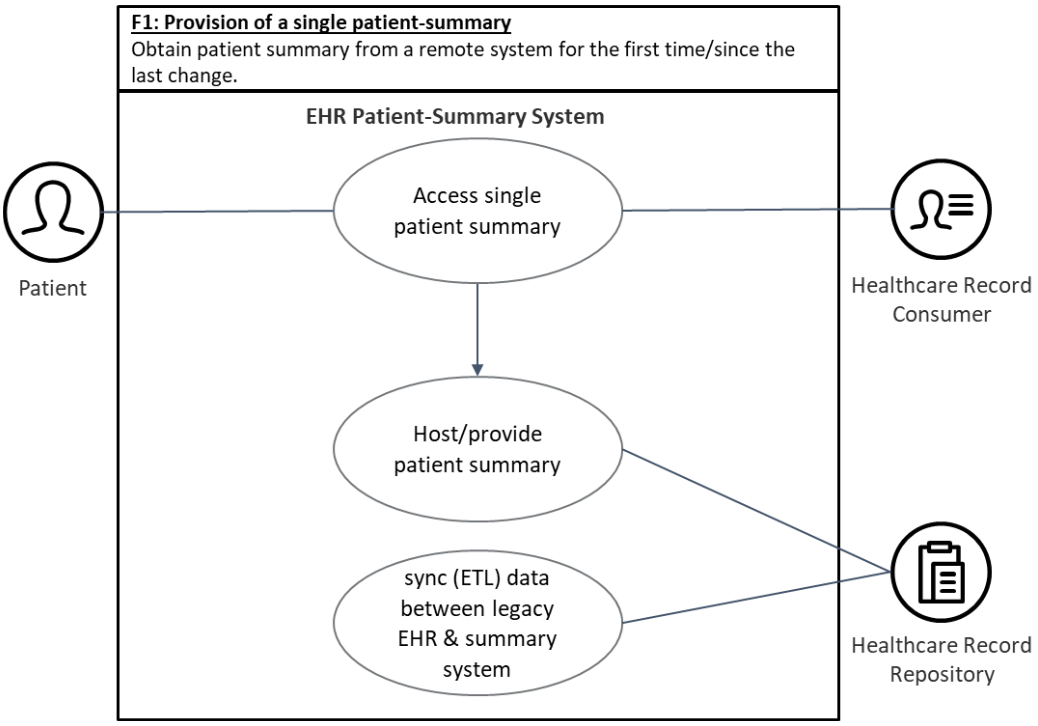
11 Appendix K – Priority Use Cases According to the eHealth Stakeholder Group report

#	Use Case	Level
1	Patient summary	national and cross border level
2	ePrescription	national and cross border level
3	Medical imaging information sharing	cross regional
4	Hospital Diagnosis Imaging Workflow	intra-hospital
5	Laboratory Information Sharing	cross regional
6	Hospital laboratory workflow	intra hospital
7	Telemonitoring of chronic diseases focusing on heart disease and diabetes	hospital / home
8	Integrated neonatal care	cross sectoral
9	Input of well-being management applications health data into medical records	N/A

12 Appendix L – Detailed Use-Case Description

ID	Use Case Name	Use Case Description	Application	Primary Actor	Precondition	Trigger	Basic Flow	Alternate flow
U1	Provision of a single patient summary	Obtain patient summary from a remote system for the first time/since the last change.	- EHR-Patient Summary System - legacy EHR system	- Patient - Healthcare Record Consumer - Healthcare Record Repository	- Patient identification properties - Location and (preferably) patient record standard of original patient record must be known. - Actors must have a valid user account in the EHR-Patient Summary System. - Healthcare Record Consumer must be authorised to access requested patient summary.	Patient or Healthcare Record Consumer requests patient summary	1. Original Patient Data is pulled from the legacy system since last change or for the first time in accordance with the cross-border directive 2011/24/EU Release 1. 2. Patient summary data is transformed to common data set and stored by the Healthcare Record Repository. 3. Patient summary is accessed by dedicated user (Patient or Healthcare Record Consumer) according to user access rights.	Alternate flow if location of patient record or Patient identification properties are unknown: 1. Patient Summary is created directly within the EHR-Patient-Summary-System in accordance with the cross-border directive 2011/24/EU Release 1. Alternate flow if actor has no valid user account: 1. User account creation is requested. 2. User account creation is reviewed. 3. User account creation is performed. 4. continuation with basic flow Alternate flow Healthcare Record Consumer is not authorised to access requested patient summary: 1. Patient summary access request is send to patient 2. Access request is granted by patient 3. Access is either granted or denied 3a. If granted, continuation with basic flow. 3b. If denied, process stops and notifies the Health Care Record Consumer about the event.
U2	Provision of multiple patient summaries	Obtain multiple patient summaries from remote system for the first time/since last change in one batch.	- EHR-Patient Summary System - legacy EHR system	- Healthcare Record Consumer - Healthcare Record Repository	- Patient identification properties - Location and (preferably) patient record standard of original patient record must be known. - Actors must have a valid user account in the EHR-Patient Summary System. - Healthcare Record Consumer must be authorised to access requested patient summary.	Healthcare Record Consumer requests patient summaries	IDEM except that several summaries are requested	
U3	Provision of previous patient summary versions and revision histories	Obtain version and revision history of a patient summary from a remote system.	- EHR-Patient Summary System - legacy EHR system	- Patients Monitoring Agent - Patient - Healthcare Record Issuer - Healthcare Record Consumer - Healthcare Record Repository	- Patient identification properties - Patient summary should have already been pulled and converted (see Use-Case 1 & 2) - Actors must have a valid user account in the EHR-Patient Summary System. - Actors must be authorised to access version & revision history.	Patient, Healthcare Record Consumer or Healthcare Record issuer requests access to the version and revision history.	1. Original change history is pulled from the legacy system 2. data is transformed to common data set and stored by Healthcare Record Repository 3. Patients Monitoring Agent monitors changes performed to healthcare summary 4. Patient Monitoring Agent provides version and revision history to patient, healthcare record issuer or healthcare record consumer.	
U4	Systematic update requests	1. Periodic update of changes to the patient summary since last change for a specified period. 2. Event driven update due to certain event on the patient summary occurred.	- EHR-Patient Summary System	- Healthcare Record Issuer - Healthcare Record Repository	- Patient summary should have already been pulled and converted (see Use-Case 1 & 2) - Actors must have a valid user account in the EHR-Patient Summary System. - Actors must be authorised to access version & revision history.	Patient summary is updated by Healthcare record issuer	1. Patient summary is already available on the patient summary system based on use-case 1 2. Healthcare record issuer is eligible of performing updates (changed, add, delete) to the patient summary 3a. Periodic update is performed due to common changes on the summary. 3b. Event driven update is performed due to changes in the patient summary 4. changes are monitored (see use-case 3.)	
U5	Access Monitoring	Provide access monitoring information according the patient summary access.	- EHR-Patient Summary System	- Patients Monitoring Agent - Patient - Healthcare Record Issuer - Healthcare Record Consumer - Healthcare Record Repository	- Patient identification properties - Patient summary should have already been pulled and converted (see Use-Case 1 & 2) - Actors must have a valid user account in the EHR-Patient Summary System. - Actros must be authorised to access version & revision history.	Patient summary is accessed by actor	1. Patient summary is already available on the patient summary system based on use-case 1 2. Patient summary access rights are defined by Patient and kept by Patients Monitoring Agent 3. Patients Monitoring Agent monitors read, write and deletion access to the patient summary 4. access attempts are logged 5. if access attempts are denied, patient gets notification and can grant/deny access.	

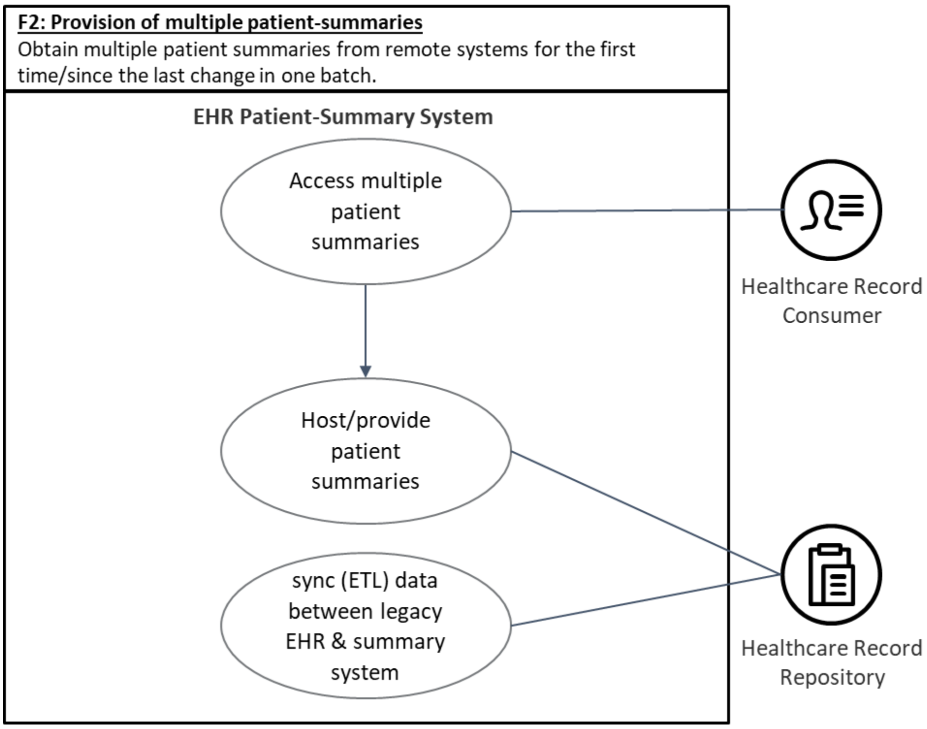
13 Appendix M – Use Case Diagrams per Scenario



F1: Provision of a single patient-summary

Obtain patient summary from a remote system for the first time/since the last change.

EHR Patient-Summary System
Access single patient summary
Host/provide patient summary
sync (ETL) data between legacy EHR & summary system
Patient
Healthcare Record Consumer
Healthcare Record Repository



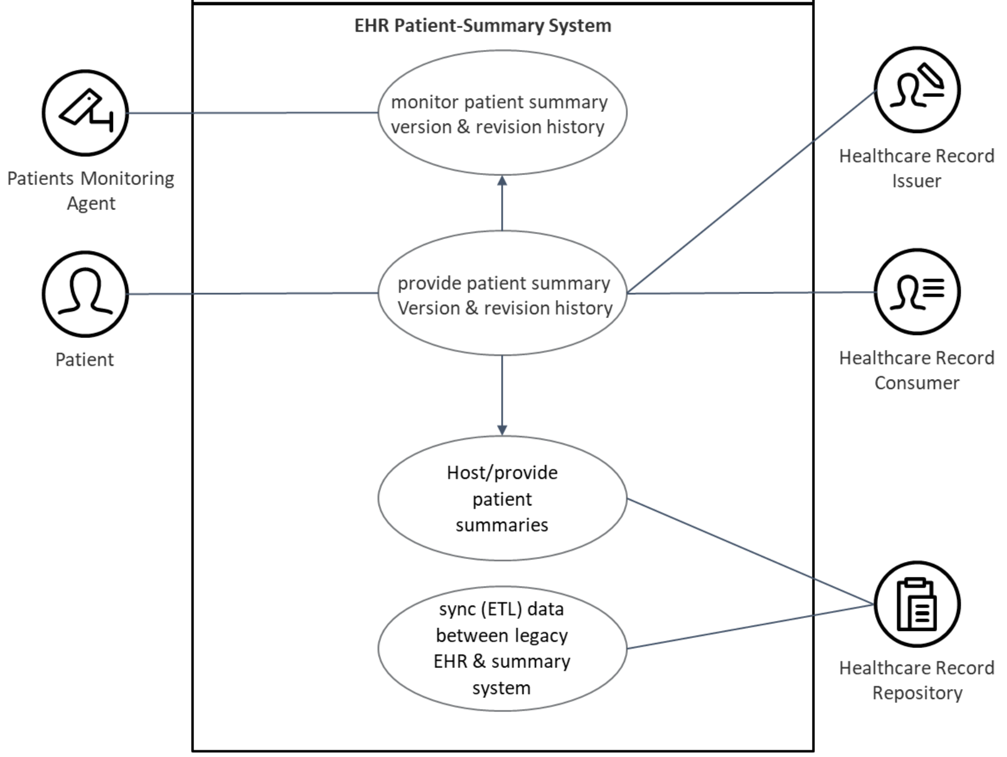
F2: Provision of multiple patient-summaries

Obtain multiple patient summaries from remote systems for the first time/since the last change in one batch.

EHR Patient-Summary System
Access multiple patient summaries
Host/provide patient summaries
sync (ETL) data between legacy EHR & summary system
Healthcare Record Consumer
Healthcare Record Repository

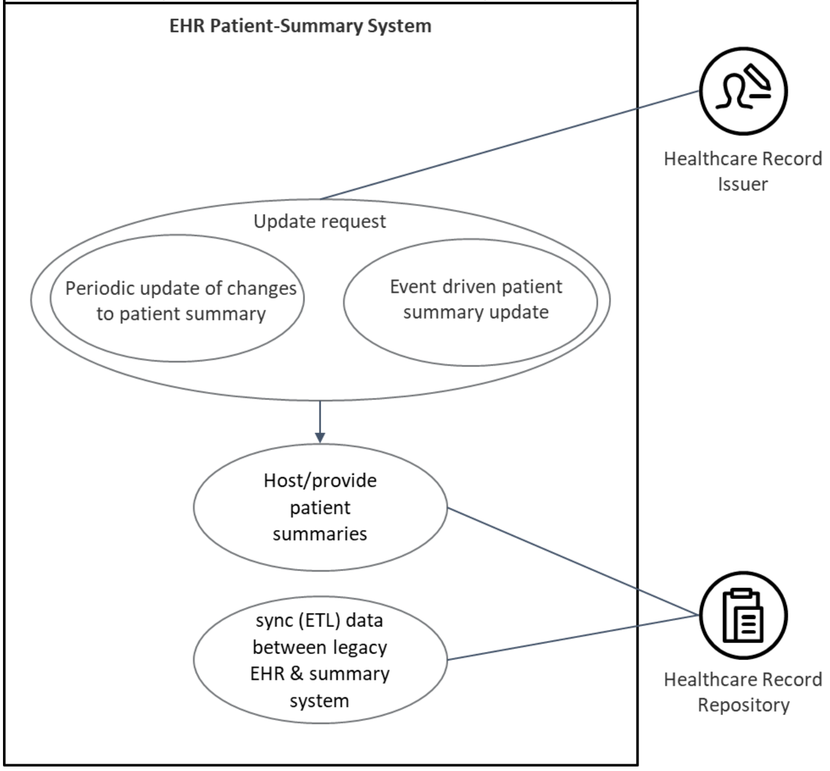
F3: Provision of patient summary version & revision

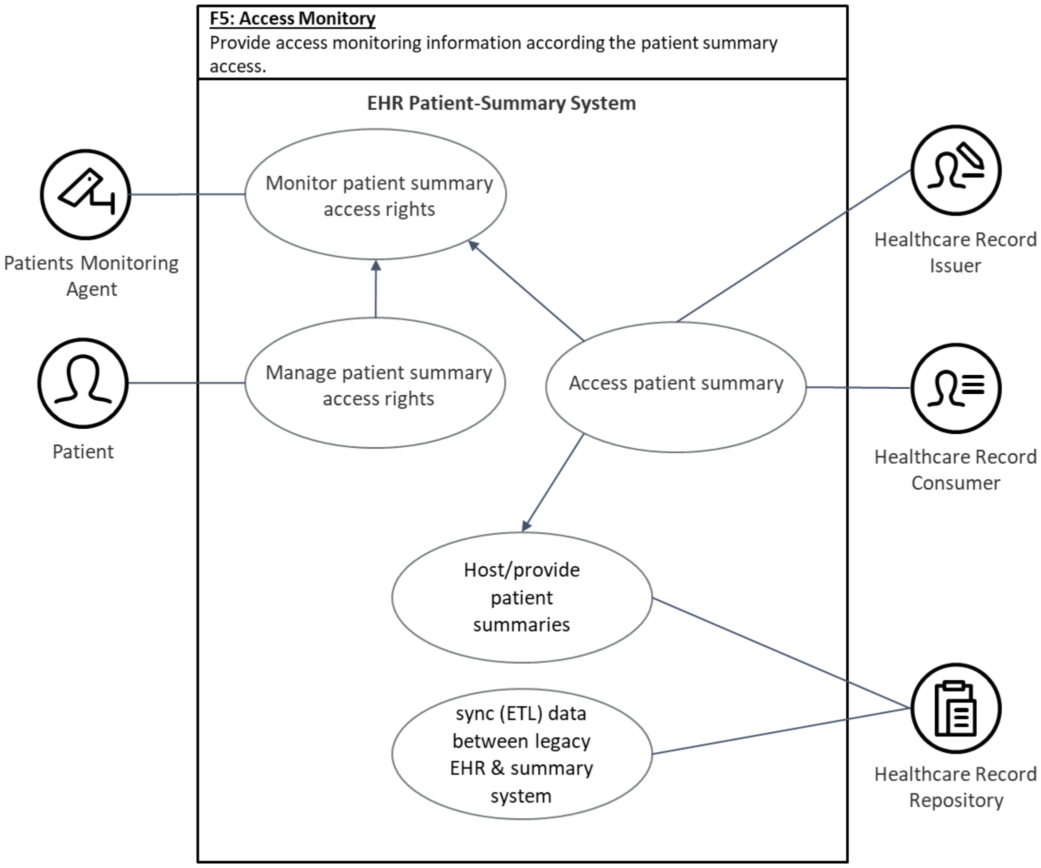
Obtain version and revision history of a patient summary from a remote system.


EHR Patient-Summary System
monitor patient summary version & revision history
Patients Monitoring Agent
provide patient summary Version & revision history
Patient
Healthcare Record Issuer
Healthcare Record Consumer
Host/provide patient summaries
sync (ETL) data between legacy EHR & summary system
Healthcare Record Repository

F4: Systematic update request

1. Periodic updates of changes to patient summary since last change for a specified period.
2. Event driven update due to certain events occurred on patient summary


EHR Patient-Summary System
Healthcare Record Issuer
Update request
Periodic update of changes to patient summary
Event driven patient summary update
Host/provide patient summaries
sync (ETL) data between legacy EHR & summary system
Healthcare Record Repository



F5: Access Monitory

Provide access monitoring information according the patient summary access.

EHR Patient-Summary System
Patients Monitoring Agent
Patient
Monitor patient summary access rights
Manage patient summary access rights
Access patient summary
Host/provide patient summaries
sync (ETL) data between legacy EHR & summary system
Healthcare Record Issuer
Healthcare Record Consumer
Healthcare Record Repository

14 Appendix N – Patient Summary Dataset

Clinical Data				
Variable (nesting level 1)	**Variable (nesting level 2)**	**Variable (nesting level 3)**	**Definition & comments**	**Basic/Extended**
Identification	National healthcare patient ID	National healthcare patient ID	Country ID, unique to the patient in that country. Example: ID for United Kingdom patient	Basic
Personal information	Full name	Given name	The first name of the patient (example: John). This field can contain more than one element	Basic
		Family name/surname	This field can contain more than one element. Example: Español Smith Note: some countries require surnames to be the birth name [to avoid potential problems with married women's surnames).	Basic
	Date of birth	Date of birth	This field may contain only the year if the day and month are not available, e.g. 01/01/2009	Basic
	Gender	Gender code	This field must contain a recognized valid value.	Basic
Contact information	Address	Street	Example: Oxford Street	Extended
		House number	Example: 221	Extended
		City	Example: London	Extended
		Post code	Example: W1W 8LG	Extended
		State or province	Example: London	Extended
		Country	Example: UK	Extended
	Telephone no.	Telephone no.	Example: +45 20 7025 6161	Extended
	e-mail	e-mail	Example: jens@hotmail.com	Extended
	preferred HP/HPO to contact	Name of the Health Professional/Health Provider	Name of the HP/ HPO that has been treating the patient. If this is an HP, the structure of the name will be the same as described in 'Full name' (given name, family name/surname).	Basic
		Telephone no.	Example: +45 20 7025 6161	Basic
		e-mail	e-mail of the HP/legal organization	Basic
	Contact person/legal guardian	Role of that person	Legal guardian or contact person	Extended
		Given name	The first name of the contact person/guardian (example: Peter). This field can contain more than one element.	Extended
		Family name/surname	This field can contain more than one element. Example: Español Smith	Extended
		Telephone no.	Example: +45 20 7025 6161	Extended
		e-mail	e-mail of the contact person/legal guardian	Extended
Insurance information	Insurance number	Insurance number	Example: QQ 12 34 56 A	Extended
Alerts	Allergy	Allergy description	Description of the clinical manifestation of the allergic reaction. Example: anaphylactic shock, angioedema (the clinical manifestation also gives information about the severity of the observed reaction)	Basic
		Allergy description ID code	Normalized identifier	Basic
		Onset date	Date of the observation of the reaction	Extended
		Agent	Describes the agent (drug, food, chemical agent, etc.) that is responsible for the adverse reaction	Basic
		Agent ID code	Normalized identifier	Basic
	Medical alert information	Healthcare alert description	Medical alert information: any other clinical information that is essential to know so that the life or health of the patient does not come under threat. Example 1: Intolerance to aspirin due to gastrointestinal bleeding. Example 2: intolerance to captopril because of cough (the patient is not allergic but cannot tolerate it because of persistent cough).	Basic
		Healthcare alert ID code	Normalized identifier	Basic
Medical history	Vaccinations	Vaccinations	Contains each disease against which the patient has been immunized	Extended
		Brand name		Extended
		Vaccination ID code	Normalized identifier	Extended
		Vaccination date	Date when the immunization was given	Extended
	List of resolved, closed or inactive problems	Problem description	Problems or diagnoses not included in the definition of "current problems or diagnosis". Example: hepatic cyst (the patient has been treated with an hepatic cystectomy that solved the problem, which is therefore a closed problem)	Extended
		Problem ID code	Normalized identifier	Extended
		Onset time	Date of onset of problem	Extended
		End date	Problem resolution date	Extended
		Resolution circumstances	Describes the reason for which the status of the problem changed from current to inactive (e.g. surgical procedure, medical treatment, etc.). This field includes "free text" if the resolution circumstances are not already included in other fields such as surgical procedure, medical device, etc., e.g. hepatic cystectomy (this will be the resolution circumstances for the problem "hepatic cyst" and will be included in surgical procedures).	Extended
	Surgical procedures prior to the past six months	Procedure description	Describes the type of procedure	Basic
		Procedure ID (code)	Normalized identifier	Basic
		Procedure date	Date when procedure was performed	Basic
Medical problems	List of current problems/diagnoses	Problem/diagnosis description	Problems/diagnoses that fit these conditions: conditions that may have a chronic or relapsing course (e.g. exacerbations of asthma, irritable bowel syndrome), conditions for which the patient receives repeat medications (e.g. diabetes mellitus, hypertension) and conditions that are persistent and serious contraindications for classes of medication (e.g. dyspepsia, migraine and asthma)	Basic
		Problem ID (code)	Normalized identifier	Basic
		Onset time	Date of onset of problem	Basic
	Medical devices and implants	Device and implant description	Describes the patient's implanted and external medical devices and equipment upon which their health status depends. Includes devices such as cardiac pacemakers, implantable fibrillators, prostheses, ferromagnetic bone implants, etc. of which the HP needs to be aware.	Basic
		Device ID code	Normalized identifier	Basic
		Implant date	Date when procedure was performed	Basic
	Major surgical procedures in the past six months	Procedure description	Describes the type of procedure	Basic
		Procedure ID (code)	Normalized identifier Date	Basic
		Procedure date	Date when procedure was performed	Basic
	Treatment recommendations	Description of recommendations	Therapeutic recommendations that do not include drugs (diet, physical exercise constraints, etc.)	Basic
		Recommendation ID (code)	Normalized identifier	Basic
	Autonomy/invalidity	Description	Need for the patient to be continuously assessed by third parties; invalidity status may influence decisions about how to administer treatments	Basic
		Invalidity ID code	Normalized invalidity identifier (if any, otherwise free text)	Basic
Medication summary	List of current medicines	Active ingredient	Substance that alone or in combination with one or more other ingredients produces the intended activity of a medicinal product. Example: "paracetamol"	Basic
		Exemption: brand name	Brand name if a biological medicinal product or when justified by the health professional (ref. Commission Directive 2012/52/EU)	Basic
		Active ingredient ID code	Code that identifies the active ingredient	Basic
		Strength	Content of the active ingredient expressed quantifiably per dosage unit, per unit of volume or per unit of weight, according to the pharmaceutical dose form. Example: 500 mg per tablet	Basic
		Pharmaceutical dose form	Form in which a pharmaceutical product is presented in the medicinal product packaging (e.g. tablet, syrup)	Basic
		Number of units per intake	Number of units per intake that the patient is taking. Example: 1 tablet	Basic
		Frequency of intakes	Frequency of intakes per hour/day/week/month. Example: every 24 hours	Basic
		Duration of treatment	Example: 14 days	Basic
		Date of onset of treatment	Date when patient needs to start taking the medicine prescribed	Basic
Social history	Social history observations	Social history observations related to smoking, alcohol and diet	Health-related "lifestyle factors" or "lifestyle observations" Example: cigarette smoker, alcohol consumption	Extended
		Reference date range	Example: from 1974 to 2004	Extended
Pregnancy history	Expected date of delivery	Expected date of delivery	Date on which the woman is due to give birth. Year, month and day are required (e.g. 01/01/2014).	Extended
Physical findings	Vital signs observations	Blood pressure	One blood pressure value, which includes systolic blood pressure and diastolic blood pressure	Extended
		Date when blood pressure was measured	Date when blood pressure was measured	Extended
Diagnostic tests	Blood group	Result of blood group	Result of blood group test performed on the patient	Extended
		Date	Date on which the blood group test was performed. This field may contain only the year if the day and month are not available (e.g. 01/01/2009).	Extended
Patient Administrative Data				
Country	Country	Country	Name of country A	Basic
Patient Summary	Date created	Date created	Date on which Patient summary was generated	Basic
	Date of last update	Date of last update	Date on which Patient summary was updated (date of most recent version)	Basic
Nature of Patient Summary	Nature of Patient Summary	Nature of Patient Summary	Defines the context in which it was generated. Distinguishes between three methodological approaches for generating the PS: direct human intervention by an HP, automatically generated approach and mixed approach.	Basic
Author organisation	Author organisation	Author organisation	At least one author organization (HCP) shall be listed. If there is no HCP, at least HP shall be listed.	Basic

15 Appendix O – Detailed Class Diagram Description

a. Extract_Package

Package	**Extract_Package**	
Class	openEHR_EXTRACT	
Description	Type of EHR_EXTRACT_ITEM containing openEHR compliant attributes to query (openEHR) legacy systems properly to obtain patient data. The class is assigned to protected visibilities to assure accessibility only by its inherit class.	
Inherit	EXTRACT_ITEM	
Attributes	**Signature**	**Meaning**
	Item: #openEHR_OBJECT_ID Item: #ORIGINAL_openEHR_VERSION	- Unique identifier of openEHR object items - Content obtained from legacy system
Function	#get_openEHR_DATA()	- Function call in order to trigger the data extraction process for openEHR related EHR systems.
Class	GENERIC_EXTRACT	
Description	Type of EHR_EXTRACT_ITEM containing generic attributes to query any EHR legacy systems properly to obtain patient. Class is assigned to protected visibilities to assure accessibility only by its inherit class.	
Inherit	EXTRACT_ITEM	
Attributes	**Signature**	**Meaning**
	Item: #EHR_OBJECT_ID Item: #ORIGINAL_GENERIC_VERSION	- Unique identifier of any EHR object item - Content obtained from legacy system
Function	#get_genericEHR_DATA()	- Function call in order to trigger the data extraction process for EHR data of any (non-openEHR) EHR systems.
Class	EXTRACT_ITEM	
Description	Abstract class of a wrapper for the items obtained from the legacy system. Contains various meta-data and patient related data. Class is only accessible within the Extract_Package due to its defined ~visibility.	
Attributes	**Signature**	**Meaning**
	Item: ~EXTRACT_ITEM_ID Item: ~EXTRACT_ITEM	- Unique identifier of items/content obtained - Items extracted, organised per chapter
Function	~create_extract_chapter()	- creates chapter for the obtained data in order to assure a proper versioning of the extracted data
Class	EXTRACT	
Description	Generic class of an extract of information obtained from various kinds of legacy systems. Class can only be accessed within the Extract_Package.	
Attributes	**Signature**	**Meaning**
	Item: ~EXTRACT_ID Item: ~time_created Item: ~system_id	- Unique identifier for the extract represented in class - Creation time of extract - Unique identifier for the system the data has been obtained from.
Class	EXTRACT_SPECIFICATION	
Description	Specifies the extract and describes what is contained in the extract. Function of the class can only be accessed within the Extract_Package and attributes only by the class itself	
Attributes	**Signature**	**Meaning**
	Item: -EXTRACT_SPECIFICATION_ID Item: -extract_type Item: -priority (1 – 3) Item: -other details	- Unique identifier for the extract specification - Indication for a full or update request - Extract priority indication, 1 = low, 2 = medium, 3 = high - Additional details which can be added relevant for the extract and created based on Archetypes
Function	~specify_extract()	- Function enabling the specification of an extract request
Class	EXTRACT_REQUEST	
Description	Generic class of a request for an extract containing extract specifications. Class accessed within the Extract & Mapping Package due to its protection visibility.	
Inherit	GENERIC_ENTRY	
Attributes	**Signature**	**Meaning**
	Item: #EXTRACT_REQUEST_ID	- Unique identifier for the extract requests performed created by the requestor.
Function	~requestDATA()	- Function to start the request process.

Table 41: Description – Extract_Package

b. Mapping Package

Package	**Mapping_Package**	
Class	GENERIC_ENTRY	
Description	Class to create intermediate representation of data from various openEHR & non-openEHR legacy systems. The class is only accessible within the Mapping_Package.	
Attributes	**Signature**	**Meaning**
	Item: ~GENERIC_ENTRY_ID Item: ~CONTENT_ITEM	- Unique identifier for the generic entry - Content containing the obtained (raw) data
Function	~Create_content_item()	- Function in order to create the content in a container obtained from the extract request
Class	COMPOSITION	
Description	Class containing the modified patient summary data based on openEHR related archetypes. The class is accessible within the Mapping_Package and through the SmartContract_Package.	
Inherit	PATIENT_SUMMARY	
Attributes	**Signature**	**Meaning**
	Item: COMPOSITION_ID Item: archetyp_ID	Unique identifier need for the versioning of the created composition Archetype identifier
Function	- create_patient_summary() # provide_patient_summary()	- Function in order to create the patient summary in line with the openEHR reference model - Provision of the patient summary due to the protected visibility to the PATIENT_SUMMARY class
Class	ARCHETYPES	
Description	Class managing the Archetypes involved to create the desired patient summary.	
Attributes	**Signature**	**Meaning**
	Item: Archetype_ID	Unique identifier of Archetypes
Class	SEMANTIC_ARCHETYPES	
Description	Class responsible for the terminology mapping according to the openEHR reference model.	
Inherit	ARCHETYPES	
Attributes	**Signature**	**Meaning**
	Item: #SEMANTIC_ARCHETYPE_ID Item: #TERMINOLOGY_SERVICE	- Unique identifier for the semantic archetypes being used - Mapping service for clinical models to meet the openEHR reference model. Note, that mapping rules need to be defined manually before they can be implemented. According to openEHR, the application: LinkEHR can be used.(Maldonado et al., 2011)
Function	#map_terminology()	- Function in order to map the desired clinical terminology
Class	SYNTACTIC_ARCHETYPES	
Description	Class responsible for the syntactical mapping according to the openEHR reference model.	
Inherit	ARCHETYPES	
Attributes	**Signature**	**Meaning**
	Item: #SYNTACTIC_ARCHETYPE_ID Item: #DATA_VALUE	- Unique identifier for the syntactic archetypes being used - Attribute in order to map legacy data to openEHR compliant data values
Function	#map_syntactic()	- function to map desired syntax
Class	PATIENT_SUMMARY_ARCHETYPE	
Description	Archetype entailing the desired data set according to the openEHR reference model.	
Inherit	ARCHETYPES	
Attributes	**Signature**	**Meaning**
	Item: #PATIENT_SUMMARY_ARCHETYPE_ID Item: #DATA_SET_REQUIREMENTS	- Unique identifier of Patient Summary Archetype - Data set requirements defined within the archetype
Function	#define_patient_summary()	- Function in order to create the patient summary according to the openEHR reference model.

Table 42: Description - Mapping_Package

c. Smart Contract Package

Package	**SmartContract_Package**	
Class	SMART_CONTRACT	
Description	Class acting as an interface between the blockchain and the prepared patient summary in line with the openEHR reference model. Accessiblity to this class is only accessible within the SmartContract_Package.	
Attributes	**Signature**	**Meaning**
	Item: ~SMART_CONTRACT_ID Item: ~SMART_CONTRACT_NAME Item: ~SMART_CONTRACT_DETAILS	- Unique identifier for the Smart Contract - Name related to the Smart Contract interacting with the Blockchain - Smart Contract Meta Data to provide a sufficient revisioning.
Function	~ get_transactions() ~ push_patient_summary() ~ initiate request()	- Function in order to obtain all change related transactions from the Blockchain to assure that changes were performed according to the defined user access management - Function to upload the created patient summary to the Blockchain - Function to initiate the extraction request for a patient summary
Class	USER_PERMISSION	
Description	Super class in charge for the user access management applied on the patient summary. Access rights are assigned to the SmartContract_Package.	
Attributes	**Signature**	**Meaning**
	Item: ~USER_PERMISSION_ID Item: ~EHR_access_ID	- Unique identifier for the user permissions applied - Link to the EHR access class
Class	PATIENT_SUMMARY	
Description	Class containing the created patient summary interacting with the smart contract. Access rights are assigned to the SmartContract_Package	
Attributes	**Signature**	**Meaning**
	Item: ~PATIENT_SUMMARY_ID Item: ~PATIENT_SUMMARY	- Unique identifier for the dedicated patient summary. - Patient summary content.
Class	TRANSACTION_MONITORING	
Description	Class responsible for the overall change management and user access monitoring, both from the blockchain and the proposed architecture. Access and change violations are going to be identified based on this class.	
Attributes	**Signature**	**Meaning**
	Item: #TRANSACTION_MONITORING_ID Item: #versioned_object_ID	- Unique item for the transaction monitoring - Reference to the monitoring package and the data gathered based on the converting operation

Table 43: Description - SmartContract_Package

d. Access Management Package

Package	**AccessManagement_Package**	
Class	EHR_ACCESS	
Description	EHR-wide access control class. All access decisions to data in the EHR must be made in accordance with the policies and rules in this object. Class is inherited by the USER_PERMISSOINS class and therefore accessible form the SmartContract- and AccessManagement_Package.	
Inherit	USER_PERMISSIONS	
Attributes	**Signature**	**Meaning**
	Item: #EHR_ACCESS_ID Item: #session_ID	- Unique access control settings for this instance - Session identifier for monitoring purposes
Function	~createSession() ~deleteSession()	- Function to create a session depending on the assigned role - Function to delete a session depending on the assigned role

Class	USER	
Description	Entity representing all users operating in the proposed system. Access to this class is only granted within the package.	
Attributes	**Signature**	**Meaning**
	Item: ~USER_ID Item: ~USER_NAME Item: ~role_ID	- Unique identifier for user - User name description - Assigned role(s)
Function	~assignRole() ~deassignRole() ~createUserID() ~deleteUserID()	- Function to assign roles to the user account - Function to deassign role to the user account - Function to create user account - Function to delete user account

Class	SESSION	
Description	Instance to manage the assigned user sessions containing the User ID and assigned Roles depending on the operation. Class is only accessible within the AccessManagement_Package.	
Attributes	**Signature**	**Meaning**
	Item: ~SESSION_ID Item: ~SESSION_NAME Item: ~role_ID Item: ~user_ID	- Unique identifier for assigned session - Session description - Assigned roleID per session - Assigned UserID per session
Function	~addActiveRole() ~dropActiveRole() ~checkAccess() ~invokeOperation()	- Function to add a role to a user account - Function to remove a role to a user account - Function to check user access permissions - Functions to force an operation independent of the assigned roles (emergency scenario)

Class	ROLES	
Description	Instance responsibe for managing defined roles according to defined permissions. Class is only accessible within the AccessManagement_Package	
Attributes	**Signature**	**Meaning**
	Item: ~ROLE_ID Item: ~ROLE_NAME Item: ~permission_ID	- Unique role identifier - Role description - Reference to assigned permission
Function	~grantPermission() ~evokePermission() ~createRole() ~deleteRole()	- Function to grant permission to a role - Function to remove permission from a role - Function to create a new role - Function to delete a role

Class	PERMISSION	
Description	Class in order to manage permissions based on the combination of objects and operations.	
Attributes	**Signature**	**Meaning**
	Item: ~PERMISSION_ID Item: ~PERMISSION_NAME	- Unique identifier for a permission - Description name of a permission
Function	~createPermission() ~deletePermission() ~updatePermission()	- Function to create new permissions - Function to delete existing permissions - Function to update existing permissions

Class	OBJECTS	
Description	Class responsible to define the objects being accessed by the user. This could i.e. the whole patient summary or only a part of it such as the contact section.	
Inherit	PERMISSION	
Attributes	**Signature**	**Meaning**
	Item: #OBJECT_ID Item: #OBJECT_NAME	- Unique identifier of the object - object description

Class	OPERATIONS	
Description	Class responsible for managing the operations executed on objects such as: read, write, update	
Inherit	**PERMISSION**	
Attributes	**Signature**	**Meaning**
	Item: #OPERATIONS_ID Item: #OPERATIONS_NAME	- Unique identifier for the operation - Unique identifier for the operations name

Table 44: Description - AccessManagement_Package

e. Monitoring Package

Package	**Monitoring_Package**	
Class	VERSIONED_OBJECT	
Description	Class keeping a variety of extracts from blockchain transactions, user access and change management procedures. Accesssible by the Monitoring and SmartContract_Package.	
Inherit	TRANSACTION_MONITORING	
Attributes	**Signature**	**Meaning**
	Item: ~VERSIONED_OBJECT_ID	- Unique identifier of serialised versioned objects
Class	VERSIONED_ACCESS	
Description	Class maintaining a change history of granted access permissions.	
Inherit	VERSIONED_OBJECT	
Attributes	**Signature**	**Meaning**
	Item: #VERSIONED_ACCESS_ID Item: #ACCESS_HISTORY	- Unique identifier of the versioned access logged - Description of the logged user access permissions
Function	~version_UserAccess()	- Function to perform the versioning of the provided access details
Class	VERSIONED_COMPOSITION	
Description	Class responsible to track the composition history for medico-legal reasons.	
Inherit	VERSIONED_OBJECT	
Attributes	**Signature**	**Meaning**
	Item: #VERSIONED_COMPOSITION_ID Item: #COMPOSITION_HISTORY	- Unique identifier for the logged compositions - Content of the logged composition
Function	~version_composition()	- Function to obtain the compositions and create a serialised composition
Class	VERSIONED_STATUS	
Description	Class responsible to manage the status of the extraction requests in order to identify if the request is new and therefore a full request is needed or only an update since the last request.	
Inherit	VERSIONED_OBJECT	
Attributes	**Signature**	**Meaning**
	Item: #VERSIONED_STATUS_ID Item: #STATUS_HISTORY	- Unique identifier for the extraction status - Version history of extract requests performed
Function	~version_extract_status()	- Function to create the extraction status.

Table 45: Description - Monitoring_Package

16 Appendix P: Generated and Prioritised Stakeholder Scenarios

Nr.	Scenario	Quality Attribute	scenario type	received votes
1	A party has broken the cryptographic key, potentially all private health data is publicly available.	Security & Privacy	use-case	1
2	Changes in terminology/code/definitions within healthcare should be able do be updated and be available for all using parties at once.	Performance	growth	0
3	The Blockchain protocol becomes outdated or obsolete. A new one is needed, and it should be possible to do this transition relatively smooth.	Evolution	exploratory	7
4	Who pays for maintaining security of the blockchain? Incentive? Decentralised? Centralised?	Evolution	exploratory	3
5	Encryption keys are lost, potentially all data is lost.	Security & Privacy	exploratory	6
6	Once a new system/hospital/country wants to use the architecture it should be possible to integrate them easily within short time.	Communication	growth	4
7	A user might not want to share health data with every health record consumer, but only specific ones or exclude specific areas.	Security & Privacy	use-case	1
8	Every good solution should be built on already existing standards, are there standards?	Communication	use-case	0
9	Demographic: number of people over 90years old. Growth fast: more people in the system with more treatments/data.	Performance	growth	1
10	The ehealth system is supposed to be used across the EU. It is possible that countries might join or leave the EU. The system should be scalable.	Performance	growth	3
11	Access to anonymous statistical data for research purposes.	Security & Privacy	growth	2
12	Collapse of the economic system, massive increase of number of refugees. Very frequent change of doctor.	Performance	exploratory	0
13	New information/function produced by (group of) owner should be able to implement without any discomfort for other non-users.	Performance	growth	0
14	Medical centre updates the database scheme -> incentive updating the mapping	Evolution	growth	0
15	A doctor try's to access medical data from his ex-wife, he should be denied.	Security & Privacy	use-case	2
16	A Hospital wants to opt. out of the current system and wants to go "standalone".	Evolution	growth	1
17	Children and maybe patients with a mental health disorder could/should need a co-owner in order to have clear insight about their medical situation.	Medico-Legal	use-case	1
18	After the death of a patient, his kids wants all data to be deleted. Who has the authority to decide? He had no other family. (what happens to the data if it is not in a will?)	Medico-Legal	use-case	2
19	Patient moves to another country and breaks his leg. The hospital should have access to his data at home	Communication	use-case	1
20	Patient has lost trust in the doctor and his/her diagnose and wants all references to this removed before going to new hospital.	Medico-Legal	use-case	0
21	When patients are unsure about certain medical decisions it might be useful for them to communicate with other owner that experienced similar situation.	Communication	use-case	0
22	A sceptical patient wants to opt-out of the her entirely. About 15 years worth of data currently stored.	Medico-Legal	use-case	0
23	A mistake was made in the records, i.e doctor made an error. Do you delete from the chain or how do you deal with this?	Medico-Legal	use-case	3
24	the blockchain uses encryption to store sensitive data? Who is responsible for the private keys?	Security & Privacy	growth	0
25	A member state privatises their healthcare and opens up medical data to insurance company. Could be illegal for other countries, how is this handled?	Medico-Legal	growth	2