UNIVERSITY OF TWENTE.

Analysing the information technology and security risks of Epic

The difference in the risk perception of Epic between the literature and practice

Mei Li Go

September 5, 2023

Supervisors University of Twente:
dr. R. Effing
dr. M. Daneva
Supervisors KPMG:
M. Fakirou
P. Tiekstra

Faculty of Electrical Engineering, Mathematics and Computer Science
Faculty of Behavioural, Management and Social Sciences
University of Twente
The Netherlands

Abstract

Electronic Health Records systems are one of the most vital systems in hospitals, containing all the medical records of its patients. Without it, hospitals are unable to properly care for their patients and patient lives could be endangered. The information technology and security risks of such a system should therefore be well known, both in literature and in practice. This qualitative study determined the difference between the perceived risks of Electronic Health Records systems in literature and in practice. It focused on hospitals in the Netherlands using the Electronic Health Records system Epic. Epic was selected as it is the second-largest Electronic Health Records system provider for Dutch hospitals. In this study a systematic literature research was conducted, as well as semi-structured interviews with hospital staff members who provide operational support to the system. The aim of this study was not only to determine the differences between literature and practice, but also to determine the shortcomings that both (literature and hospitals) have in their risk perception. The results show that the literature focuses more on the risks in papers, such as the risk of not having a security protocol. In contrast, interview participants focused on the risks that occur when IT is done in practice. Literature also fails to give the full context of a risk, only giving a general description with worst-case scenarios to illustrate the impact a risk can have. Participants, on the other hand, provided detailed descriptions of risks. They explained how and why a risks manifested, and gave examples of risk manifestations that did not have a severe impact but did occur often. Next to that, participants stated which measures hospitals take to prevent risks, which was often lacking in literature. Overall, the research showed a clear difference between the perceived risks in literature and those in practice, the most important of which is that the literature lacks a detailed and accurate risk description.

Contents

Chapter 1

Introduction

An Electronic Health Records system is one of the most important systems in a hospital. It stores all information concerning the hospitals' patients in digital records and allows this information to be shared among different healthcare providers and to the patient (Hoerbst and Ammenwerth, 2010; McMullen et al., 2014). A failure of this system can have catastrophic consequences and endanger the health of patients. For example, a hospital in Maastricht had to cancel the treatment of thousands of patients due to a malfunction of their Electronic Health Records system (Verkerk, 2022). Moreover, a hardware failure in the Queensway Carleton Hospital caused patient data to be inaccessible and equipment to become inoperable. This endangered patients as, among other things, the bed alarms stopped working. Additionally, privacy regulations were violated as doctors started requesting patient data using their personal cellular phone coverage (Anad and Chin, 2022). It is therefore important that an Electronic Health Records system is available and accessible, and that it is protected against any threats against its availability, confidentiality, and integrity. The COVID-19 pandemic also accelerated the digital transformation of hospitals, among others with video consultations, which further increased the importance of Electronic Health Records systems. With the changes to the systems and their importance, it is essential that literature gives an accurate representation of the risks associated with Electronic Health Records systems, which may not be the case due to the developments of the systems.

An important aspect of Electronic Health Records is that they are usually Commercial-Off-The-Shelf (COTS) software. COTS software is developed and maintained by an external company (the provider), and multiple companies buy a copy of the software in order to use it. This makes the hospital dependent on the provider for maintenance and upgrades of the system (Heart, 2010; Redmill, 2004; Ángel DÍaz De León Guillén et al., 2020). Moreover, as an Electronic Health Records system is also a vital system to the hospital, the hospital is unlikely to switch to a different provider, which further increases their dependency on the vendor. This is called vendor lock-in. In 2021, 76 hospital locations in the Netherlands had a COTS Electronic Health Records system, according to an M&I Partners research (van Eekeren et al., 2021). This is compared to the 113 hospital locations that were reported in the Netherlands in 2022 (RIVM, 2022), which implies that the majority of hospitals in the Netherlands use COTS software for their Electronic Health Records.

Another aspect of Electronic Health Records systems is that it is, or inevitably will become, a legacy system. Legacy systems are systems that are unable to meet the evolving

functional and security requirements of hospitals. This inability to adapt to changing requirements is due to legacy systems using outdated techniques (Bennett, 1995) and resisting modification (Brodie and Stonebraker, 1995). Moreover, experts for these techniques are sparse and costly, and maintaining the system - due to its large volume and often incomplete documentation - will become more expensive over time (Comella-Dorda et al., 2000; Bisbal et al., 1999). This is relevant, as the two main providers of Electronic Health Records system in the Netherlands, Epic and HiX, are both already over 25 years old and are legacy systems (van Eekeren et al., 2021; Chipsfot, nd; Epic, nd).

With these aspects in mind, as well as the importance of Electronic Health Records, it is essential to determine the risks of such a system in order to prevent the endangerment of patients and their data and to ensure that proper care is provided. This study focuses on the information technology and security risks of Electronic Health Records systems, and aims to determine the difference between these risks in literature and as they are perceived in practice. To determine the risks that are currently available in the literature, a literature research will be conducted. Then, staff members who provide operational support for the Electronic Health Records System Epic will be interviewed about the information technology and security risks of it. These results will be compared to each other and the differences determined. The Epic system, provided by the company Epic, was selected for this research as it is the second-largest Electronic Health Records system provider for hospitals in the Netherlands. The system is used in twelve out of 69 Dutch hospital organizations, which includes 4 out of 7 University Medical Centers (van Eekeren et al., 2021; RIVM, 2022; Amsterdam UMC, nd; Maastricht UMC, 2023; Ziekenhuis Amstelland, 2022).

1.1 Research motivation

An Electronic Health Records system is one of the most vital systems that the hospital needs to function. If this system is offline, patients can not be treated and it can cause life-threatening situations, as explained earlier. It is therefore important that hospitals are able to identify the risks of their Electronic Health Records system. However, they will need appropriate resources to do so, and literature is one of the resources they can use. The literature should therefore give an accurate representation of the risks. However, the COVID-19 pandemic has caused an acceleration in the digital transformation of the hospital, which also includes the Electronic Health Records systems (Gude and van Luxemburg, 2020). One of the improvements of the Electronic Health Records systems was, for example, the use of video consultations. It is thus important to analyze if the available literature is still accurate given the developments of Electronic Health Record systems.

Establishing the shortcomings of the risk perception in literature as well as in practice is important as both can improve hospital practices. Identifying the shortcomings of the literature gives not only hospitals but also future researchers more accurate information about Electronic Health Records systems risks. Determining the shortcomings of how hospitals perceive risk - by comparing them to the risks specified in literature - can help them create a more accurate risk understanding. The goal of this research is therefore to identify the difference in risks between literature and practice.

1.2 Research Questions

To achieve the goal of this study, the following research question has been formulated:

What are the differences between literature and the users' perception about the perceived information technology and security risks of Epic in hospitals in the Netherlands?

In this research, the users are specified as the people providing operational support for the system. Additionally, the research will only focus on the risks of an Epic system that is in use and fully implemented, and thus will not discuss any implementation risks of Epic. The reason for this is that many Dutch hospitals already use an Epic system (van Eekeren et al., 2021), and therefore these risks are the most relevant to them.

To help answer the main research question, the following sub-questions have been formulated:

1. What are the most prominent Electronic Health Records system risks in literature?
   (a) Which risks are of particular importance in relation to an Electronic Health Records System?
   (b) What are the most prominent risks of commercial-off-the-shelf (COTS) software?
2. What are the risks of Epic according to users?
   (a) In which circumstances will a risk take place?
   (b) What are the consequences of a risk-taking place?
   (c) Which risks are the greatest threat to the hospitals' operations?

1.3 Outline

This thesis has the following structure: chapter 2 describes the method in which research was conducted. chapter 3 focuses on the first sub-research question and describes the risks that are specified in the literature. In chapter 4 the risks that were found in the interviews will be described in detail, after which - in chapter 5 - these risks will be compared to the risks stated in the literature. Finally, in chapter 6 a conclusion to the research will be given. It will answer the research question as well as make suggestions for future work.

Chapter 2

Method

In this chapter, the methodology of the research will be discussed. A literature review was first conducted to create an overview of the knowledge present in research about information systems in hospitals. The literature review therefore focused on the first research question. Afterwards, interviews with experts were conducted in order to identify the risks that the experts faced using an EHR system. This will be discussed in the second section of the chapter.

2.1 Literature review

The literature research methodology is based on the methodologies presented by Webster and Watson (2002) and Wolfswinkel et al. (2013). The structure of the literature was as follows:

1. Define keywords
2. Define Queries
3. Determine Databases to search in
4. Selecting articles:
   (a) Select and read the top 4 papers based on relevance for each search term.
   (b) Select and read any other relevant papers found using the search term

Step 1: Define keywords

The keywords that were used can be found in section A.1.

Step 2: Define Queries

Based on the keywords, several queries were defined. These queries and the goal of each query is shown in Table 1 on page 9.

Step 3: Determine Databases to search in

The databases chosen were Google Scholar and Web of Science. A research by Yang and Meho (2006) found that the use of Web of Science is essential when searching for papers

Table 1: Queries

#	**Purpose of the query**	**Query**
1	Finding typical hospital information system's risks	((Hospital) OR (medical) OR (health) OR (healthcare)) AND ((Information System) OR (IS) OR (Information Technology) OR (IT) OR ((HIS) OR (HIT))) AND ((risk) OR (threat) OR (issue) OR (problem))
2	Determining what current methods for risk management are	(Risk) AND ((assessment) OR (assess) OR (evaluation) OR (management)) AND ((system) OR (software)) NOT ((project) OR (development))
3	Finding the popular software Risk Management methodologies	(Risk) AND ((evaluation) OR (management)) AND ((system) OR (software))
4	Finding typical legacy system risks	((Legacy) OR (old)) AND ((system) OR (software) OR ((information) AND ((system) OR (software)))) AND ((risk) OR (threat) OR (issue) OR (problem))
4a		Including "aging" as a keyword (synonym to legacy) to search term 4
4b		Excluding "old" as a keyword to search term 4
5	Finding the risks of COTS software	((COTS) OR (SaaS)) AND ((risk) OR (threat) OR (issue) OR (problem))
6	Finding the risks of Electronic Health Record systems	((Electronic Health Record) OR (Electronic Medical Record) OR (Electronic Patient Record) OR (Personal Health Record)) AND ((risk) OR (threat) OR (issue) OR (problem)) AND ((Information System) OR (IS) OR (Information Technology) OR (IT) OR (system))

in the information science field. Google Scholar was found to have the most extensive coverage of conference papers (Meho and Yang, 2007). Moreover, compared to only using Web of Science, including Google Scholar when searching for articles increasing the number of citations between 19-25% (Yang and Meho, 2006). Using both databases therefore results in a more accurate and comprehensive overview of papers (Meho and Yang, 2007).

Step 4: Selecting articles

Each query was searched in both Google Scholar as well as Web of Science. The results were then sorted on relevance and the top 4 articles were selected. Other articles were also selected if they were relevant, which was determined by reading the abstract of the article. The search resulted in 58 articles, which can be found in section A.2. It was found that the articles of Boehm (Boehm, 1989, 1991) were most influential on risk management methodologies. A forward search was conducted on the two articles published by Boehm to ensure that no important information was overlooked. This search resulted in the papers of Heemstra and Kusters (1996) and Taylor et al. (2012). The contents of the papers will be discussed in the next section.

2.2 Qualitative interviews

To discover which risks hospitals experience in practice, oral and semi-structured interviews were conducted. The focus of the interviews was on determining which risks the participants found important. A qualitative interviewing method was therefore chosen, namely semi-structured interviews. This type of interview uses an interview guide for the researcher. However, the order of the questions can differ from the guide and additional questions may be asked, which allows the participant to go into more detail about topics they find important (Bryman and Bell, 2015). After the interviews, the data will be analysed using the qualitative content analysis method of Kuckartz (2019). This method has six steps, namely:

1. Preparing the data
2. Forming the main categories
3. Coding the data with the main categories
4. Compiling text passages and forming subcategories
5. Category-based analysis and presenting results
6. Reporting and documentation

All the interviews were conducted over Microsoft Teams and the transcribe function will be used to gain a transcription of the interview, as part of the first step of the method. For the second step, forming main categories, the categories provided by KPMG as the co-laboratory company in this project will be used. KPMG is one of the big four auditing firms, which are four organisations that together audit a fast majority of the Fortune 500 companies (Kenton, 2022). About 227,000 people are employed at KPMG and they work in 146 countries and territories (KPMG, nda). KPMG was founded in 1917 and currently performs work for companies such as Philips (KPMG, ndb). Due to the experience of the company in auditing IT systems as well as the company's size, the categories that KPMG uses to conduct an IT audit on their clients are used in this study. These categories are used by KPMG to audit the information technology and security risk of a system, and they are as follows:

- **General Information Security**: This category does not only aim to protect the confidentiality, integrity and availability of information, but also how to deliver business benefits by both protecting and facilitating the sharing of information and managing the risks associated with it (Ashenden, 2008). KPMG mainly focuses on any processes and protocols in place to facilitate to this goal.
- **Access to programs and data**: KPMG defines this any processes and protocols in place to regulate who has access to programs and data and that they have the correct privileges.
- **Continuity**: Regards "the ability of an organization to continue to deliver products or services at an acceptable, established level in the period following a disruptive incident". Specifically, this category will focus on the business continuity management of hospitals, which is the measures that they take to be able to withstand disruptive incidents (Aleksandrova et al., 2018).

- **Change management**: For KPMG, this concerns the processes and protocols in place that document and approve any changes to the system.
- **Cyber security**: Schatz et al. (2017) defined this as "The approach and actions associated with security risk management processes followed by organizations and states to protect confidentiality, integrity and availability of data and assets used in cyber space. The concept includes guidelines, policies and collections of safeguards, technologies, tools and training to provide the best protection for the state of the cyber environment and its users."
- **Supplier management**: Is the process in which an organisation try to ensure that the maximum value is received from a supplier for the money that the organisation pays. It includes establishing a relationship with the supplier and requirement management among other things (Medius.nl, nd).

These categories will also be mentioned during the interviews and participants will be asked to determine and describe risks within the categories. Therefore the categories will correspond with the questions asked in the interview as required by the qualitative content analysis method of Kuckartz (2019). After completing the third and fourth step for each interview individually, the data gained from all the interviews will be combined and compared in step 5, and the results documented (step 6).

To find participants that have adequate knowledge about the information technology and security risks of hospitals, there are several requirements:

1. The participant has worked with Epic for at least one year
2. The participant provides operational support for the system for at least one year
3. The participant is currently providing operational support for the system

2.3 Analysing the Interviews

Five hospital staff members, covering 3 different Dutch hospitals, agreed to an interview. The participants are not end-users of Epic, but support the system and end-users. Their role descriptions are as follows:

- Participant (P) 1 and P2 manage an IT team within their hospital
- P3 helps maintaining the system and ensuring that it is available
- P4 is in contact with end-users to provide technical support
- P5 monitors and ensures the correct usage of Epic

Furthermore, the number of years the participants have worked with Epic can be viewed in Table 2.

Table 2: The years of experience working with Epic of each of the participants.

1-3	**4-6**
P1 and P4	P2,P3 and P5

The interviews were conducted in May 2023. They took approximately one hour and were conducted by video-call in Microsoft Teams. With consent of the participants, the interviews were recorded for later analysis. The interviews were also transcribed by using the transcribe function of Microsoft Teams.

For the semi-structured interviews, an interview guide was used. The guide contains 18 questions and can be found in Appendix B. The aim of the guide was to gather a detailed overview of the risks, as well as to determine if any risks had a higher priority than others . To structure the risks the six categories from KPMG were used, which are:

- General Information Security
- Access to programs and data
- Continuity
- Change management
- Cyber security
- Supplier management

In the first part of the interview ('1. Persoonlijke ervaring'), the experience and role of the participant was established. The second - and main - part of the interview focuses on which risk they encounter when working with Epic. All six categories were mentioned, and the participant was asked which ones they have the most experience with and want to focus on. The questions in this section were repeated for each category that is discussed with the participant. First, the participants was asked which risks they experienced in the last year working with Epic. Then, details about the risks they mentioned were asked, such as the circumstances in which the risk is greater, if it took place, and which processes and protocols are in place to prevent the risk. When finalising the interview, the participant was asked if they wanted to add something (question 3) and if anything was missed during the interview (question 4). These questions ensure that a participant can mention any risks that they think are important that have not been discussed yet, or add information which they think is relevant which was not discussed.

As described in the Methodology (section 2.2), the qualitative content analysis method by Kuckartz (2019) was used. The first step, preparing the data, was done by the transcription software of Microsoft Teams. The second step of forming the main categories was already completed and the categories from KPMG are used, which was also described in the methodology. Next is the step of coding the data with the main categories. This was done by using both the transcript and listening to the audio in the recordings. After the risks were coded, subcategories were formed in order to process the details of each risk. The most important subcategories are:

- *When the risks manifests*: a description of the circumstances in which a risk can happen
- *Examples*: cases in which the risk took place, or is most likely to take place. This contains a more detailed description as opposed to the first subcategory, which is a more general description of circumstances

- *Prevention*: measures that hospitals have taken to prevent the risk, and/or minimalize its' impact
- *Consequences*: a description of the impact(s) of the risk
- *Other risks*: a description of other risks that the hospital faces if the risk manifests
- *Needed to do better*: measures or resources that the hospital needs to further decrease the probability of the risk taking place

These subcategories are based on the interview script, as well as the aspects of the risk that the participants discussed the most. All subcategories can be found in Appendix D. Additionally, useful and interesting quotes where also gathered during this step.

To analyse the risks and compare the risks stated in the interviews, a mind map was made next. The mind map contained the main categories and the risks, without their description. Using the mind map, the the risks of the interviews were compared and combined if two or more participants described the same risk. The result is 29 risks which are stated in Table 9 on page 28. These risks will be discussed in the remainder of this section. Due to the large amount of risks found during the interviews, only risks that were either discussed extensively or risks named by multiple participants will be discussed in detail. The remainder of the risks will be shortly mentioned in the final subsection.

Chapter 3

Theoretical Foundation

In this section the results of the literature study will be presented. It starts by discussing the risks of a legacy information system in a hospital, followed by discussing different risk management methodologies. The success factors and shortcomings of the methodologies will also be highlighted.

3.1 Definitions

In this subsection, terms that are important to the literature research will be explained. These terms are:

- Legacy Information System
- Electronic Health Records (EHR) system
- Risk
- Commercial-off-the-shelf software (COTS)

First, a definition of a Legacy Information System will be given, which in this research is "any information system that significantly resists modification" (Brodie and Stonebraker, 1995). A Legacy Information System is often a large system, containing more than a hundred thousand lines of source code, and has a critical role in the functioning of the organisation. They are developed sometime in the past and therefore use outdated techniques (Bennett, 1995).

In a hospital context, an information system is "a comprehensive, integrated information system designed to manage the administrative, financial and clinical aspects of a hospital" (Ismail et al., 2010). The aim of such a system is to help provide high-quality health care efficiently through improving access to and storage of information, reducing errors, as well as facilitating access to relevant scientific information in decision support systems. Additionally, hospital information systems aim to lower costs and provide better time management (Borzekowski, 2009). In this research, the focus is on the Electronic Health Records (EHR) system, which is a form of a hospital information system. According to Hoerbst and Ammenwerth (2010) an EHR are "a comprehensive, cross-institutional, and longitudinal collection of a patients' health and healthcare data". An EHR system stores digital records of every health related event of a patient, and this information can be shared among different healthcare providers and to the patient (McMullen et al., 2014;

Nguyen et al., 2014; Roehrs et al., 2017)

Another important definition is that of risk. Stoneburner et al. (2002) defines risk as "A function of the likelihood of a given threat source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization.". The Society for Risk Analysis has a less pessimistic definition of risk, which can be summarized as "the relation of a future activity to its consequences with respect to something that humans value" (Aven, 2016). For this research, the definition given by Chowdhury and Arefeen (2011) will be used. They define risk as "The precursor to a problem; the probability that, at any given point in the software life cycle, the predicted goals cannot be achieved within available resources".

Lastly, Morisio and Torchiano (2002) give several definitions of COTS software from literature. All definitions have in common that it concerns pre-existing software, of which (nearly) identical copies are sold. Next to that, the source code of the COTS software is often not available and the vendor determines what is updated and the schedule of updating. The definition of Vidger and Dean (1997) will be used, which describes COTS software as pre-existing software where the customer does not have access to the source code, does not control the maintenance and evolution of the system, and the documentation of the behaviour of the system may be inadequately specified or not available.

3.2 Electronic Health Records system Risks

3.2.1 Legacy Information Systems

To answer the research question, it is important to identify the risks of a hospital Legacy Information System. To start, maintaining a Legacy Information System is often expensive. Documentation is often lacking, wherefore understanding the system and tracing faults becomes difficult and time-consuming (Bisbal et al., 1999). Next to that, legacy systems use out-of-date technology - for example a programming language that is no longer used - making it hard to find expertise. Hiring these experts is therefore not only time-consuming but, due to their skill set being relatively rare, also expensive (Comella-Dorda et al., 2000; Fürnweger et al., 2016; Adolph, 1996). A Legacy Information System is also hard to modify (Bennett, 1995; Bisbal et al., 1997, 1999; Fürnweger et al., 2016; Hussain et al., 2017). Adapting the system to new requirements or integrating it with other systems or software becomes difficult, which increases the risk that a Legacy Information System is not able to communicate and exchange data with new software that the hospital needs. This risk is further increased as Legacy Information Systems often lack interfaces which can be used to integrate the system with new software (Bisbal et al., 1999). Moreover, changing the system is not without consequences. Correcting an error is likely to introduce multiple new errors, and this will affect the system's conceptual integrity (Parnas, 1994; Comella-Dorda et al., 2000). Additionally, the system also increases in volume the longer it is in use (among other things because of an increase in files). Due to the increasing volume of the system and the demands it makes on the computer memory, the performance will degrade over time (Parnas, 1994). Furthermore, a legacy system often cannot compete with new technologies (due to the inflexibility of the system), which can result in a competitive disadvantage for the hospital (Bennett, 1995; Comella-Dorda et al., 2000; Hussain et al., 2017).

With all these risks it may seem like the best solution is to replace the system. This is, however, often a complicated and expensive operation. The costs are often difficult to estimate and there is the risk of choosing the wrong new environments, languages and setups. As a legacy information system has a critical role in the organisation it will also require extensive testing, and even then there is no guarantee that a new system will be as robust or functional as the current system (Comella-Dorda et al., 2000; Fürnweger et al., 2016). The developers of the Legacy Information System are likely not available anymore and with lacking documentation it makes it hard to understand the system and its behaviour. Therefore it becomes difficult to re-implement the software and the implicit knowledge of the system may be lost. With these risks in mind, an organisation may find it easier to maintain an existing system despite the risks. Keeping the Legacy Information System offers the hospital the advantage of preserving stability and the ability to better predict the overall system costs (Fürnweger et al., 2016). The risks discussed in this subsection can be seen in Table 3 and Table 4.

Table 3: Legacy system risks

Legacy system risks
Hard to modify
Finding experts to maintain the system is difficult and expensive
Documentation lacking
Constrained competitive advantage
Maintenance is difficult
System increasing in volume the older it gets
Correcting an error introduces more errors
Maintenance is time-consuming
Decreasing integrity
Performance degradation
Competitive disadvantage compared to new(er) technologies

Table 4: Migration risks

Migration risks
Costs are hard to estimate
Organisation chooses an environment, set up and/or language that is not suitable for their operations
Introducing bugs or unwanted software behaviour
Difficulty re-implementing the legacy system correctly as the legacy system is not fully understood
Extensive testing of new software
A new system may not be as robust or functional as the old one

3.2.2 COTS software

Other risks that hospitals face are related to their usage of COTS software, which can be found in Table 5. The source code of COTS software is rarely accessible to customers, therefore making it impossible for them to maintain or otherwise modify the system (Heart,

2010; Redmill, 2004; Ángel DÍaz De León Guillén et al., 2020). This creates an absolute dependency on the vendor for system maintenance and upgrades, which will often require additional payment. When an upgrade is released, customers have the problem that they have no input over what is included in the new version. This may result in the new version containing unwanted functionalities, being unable to communicate with other systems that the software uses without additional modifications, and there is often an increase in volume and complexity of the system. A fee may also be charged for upgrading to the new version. On top of that, the system is often 'untried' and the hospital does not know the safety implications of using this new version. If a hospital uses several COTS software provided by different suppliers there is also a possibility that the suppliers have mutually incompatible upgrades, which can be hard to manage and solve. For these reasons, a hospital can decide not to upgrade their system (Redmill, 2004; Shyur, 2006). However, this brings the complication that at some point the vendor will no longer support and maintain their version, putting the hospital in a difficult position (Redmill, 2004; Wu et al., 2006). Hospitals are also unlikely to change suppliers once they have committed to one because, in addition to the reasons named in the previous paragraph, they also have to retrain all their employees (van Lonkhuyzen, 2022). The risk of poor custom code and system performance (Shyur, 2006) results in the risk of an unavailable system, as it could cause network instability and become vulnerable to attacks among other things (Heart, 2010). These risks will be discussed in further detail in the next subsection.

Table 5: COTS software risks

COTS software risks
Black-box
Dependence on providor for maintenance
Undesirable/dangerous effects with update
No evidence/documentation
Increased financial cost
Maintenance and support only if frequent updates are done
No support for older version
No control over composition upgrades
Increased volume and complexity with each update
Asynchronous updates
Poor custom code
Poor performance
Risk of unavailability
Safety implications of the software and/or it's updates are not clear
Malicious employees and experts
Password stealing
Attack from a user, software, or the internet
Data scavenging
Data loss or leakage

3.2.3 EHR Systems

There are also risks related to the usage of an EHR system. As the system stores a special category of data from individuals, namely medical information (European Parliament and

Council of the European Union, 2016), security measures should be in place in order to prevent the system from being compromised. To create an overview of these risks, 4 categories have been created: integrity, confidentiality, data security, and content.

Integrity

Starting with the risks that concern the integrity of the data. Integrity means that the data in a system is accurate and has not been manipulated intentionally or unintentionally by the system or an unauthorized party (Hoerbst and Ammenwerth, 2010; Harman et al., 2012). To prevent unauthorized parties from reading and possibly adjusting the data in the system, data and messages from the system should be encrypted (Harman et al., 2012; Rahman and Kreider, 2012; Hoerbst and Ammenwerth, 2010; Kierkegaard, 2011) . Audit logs should be kept in order to check whether the integrity of the system has been compromised. These logs should track which data was modified, by whom, and when. It should also track who viewed or otherwise accessed the data. This tracking will make it possible to track if integrity is compromised and to which degree, and makes it possible to restore the affected data. However, integrity can also be threatened by the system itself. In the Albert Schweitzer hospital medical records of 212,000 patients were adjusted due to a system error. The error caused their files to be (partially) overwritten with new information (ICT&health, 2022). Proper maintenance and fault detection is therefore also important to ensure integrity .

Confidentiality

Next, it is important that data remains confidential, meaning that only authorized individuals have access to the data (Harman et al., 2012). To ensure confidentiality EHR systems need to have authorization and access protocols, of which the hospital staff should also be aware (Hoerbst and Ammenwerth, 2010; Kierkegaard, 2011; McMullen et al., 2014; Roehrs et al., 2017; Rahman and Kreider, 2012; Schiza et al., 2016). Access control should be role based, which allows users of the system to have varying levels of access and privileges. One of the access control rules should be, for example, that hospital staff only has access to the medical records of patients they are treating. An incident at the Haga hospital demonstrates the importance of role based access control. When a reality show personality called Barbie was hospitalized there, dozens of staff members that were not part of her treatment team accessed her medical records unauthorized. Next to disciplinary action against the staff members that viewed the medical records unauthorized, it also resulted in a fine of 350,000 euros for the Haga hospital as it was determined that they handled Barbies' medical records carelessly (NOS Nieuws, 2018, 2019; RTL Nieuws, 2018). This case also shows the importance of logging, as it allowed the hospital to determine whom accessed her records . "Die is specifiek gericht op relevante maatregelen rondom logging, zoals het maken, bewaren, inzien en structureel controleren hiervan. Dit zou een sterke toevoeging zijn op het argument dat je geeft, dat logging belangrijk is.". Moreover, it shows another important procedure that a hospital should have: to verify that each of user account in the EHR system is linked to a specific hospital staff member. An EHR system is large and complex, and there is a need for certain staff members to have additional privileges. For example, members of the IT department may need to be able to give staff members (additional) access privileges. There should be an up-to-date list with the users accounts and linked staff members who have additional privileges, to allow the hospital to verify who had additional privileges and if it is justified . Finally, in order to

keep data confidential it is important that a secure data transport protocol is in place, such that an unauthorized user can not get access to the data while it is transported.

Data security

Data security has a vital role in ensuring the system's confidentiality, integrity and availability . It can be split into three categories: insider threat, outsider threats, and protocols and procedures.

Insider threats are defined as the risks of intended damage on a system caused by authorized users of the system (Rahman and Kreider, 2012). Rahman and Kreider (2012) divides insider threats into three subcategories:

- Insider curiosity: Access privileges are abused by medical staff
- Insider subornation: An authorized user of the system intentionally accesses information and shares it with outsiders (in other words, an authorized user causes a data leak)
- Accidental disclosure: unintentional mistakes which may result in the disclosure(s) of sensitive information.

Both insider curiosity and insider subornation can be caused by disloyal and disgruntled employees (McMullen et al., 2014; Harman et al., 2012). The Bravis hospital had to deal with a case of insider curiosity and subornation when one of their hospital staff, a secretary at the emergency care department, released confidential patient information. The secretary had repeatedly looked into the medical records of her partner's ex girlfriend over the course of 4 years. Her partner then published a book that included this medical information. The secretary had access to this information because she worked at the emergency care department, and as such had unrestricted access to patients' medical records. Although the hospital had immediately fired the secretary upon the discovery of what she had done, a judge found that the hospital had failed to protect the patients' information and ordered the hospital to pay a compensation to the victim (the ex girlfriend) (Wester, 2022). This case shows the possible consequences of insider curiosity and subornation: a breach of confidentiality. The court case about the incident also determined that a hospital is liable if they do not take the appropriate measures to prevent insider curiosity and subornation (in this case their regulation of the access controls was insufficient). Next to the insider threats from the hospital staff, there is also an insider threat from third parties. Third parties with access to the EHR system, for example pharmacies, may use medical records to gain a competitive advantage (Schiza et al., 2016) . However, this is not the only way in which the integrity, confidentiality and availability of the system may be compromised. It may also occur with accidental disclosures, which can happen when a laptop, phone or other device that has access or is connected to the EHR system is left unattended and stolen as a result (Kierkegaard, 2011; McMullen et al., 2014; Harman et al., 2012; Rahman and Kreider, 2012; Raposo, 2015). Other ways in which accidental disclosures may happen is if a doctor forgets to log out of a shared computer resulting in another person having access to their account, or medical staff accidentally sending an email containing confidential information to the wrong email address. Poor password management can also be a cause of an accidental disclosure. Preventing accidental disclosures is important as the healthcare sector has one of the highest data leak report percentages.

In 2019 28% of the data leak reports was from the healthcare sector, of which 25% was from hospitals (Autoriteit Persoonsgegevens, 2020). In 2021 the health and well being sector accounted for 37% of the data leak reports, which totals 9,200 reports (Autoriteit Persoonsgegevens, 2022). The high data leakage percentage of the sector shows that more improvements and prevention measures are necessary.

The second type of threat against data security is external threats. This is the risk of an unauthorized user wanting to damage the system, threatening the integrity, confidentiality and availability of the system (Rahman and Kreider, 2012). This can happen when someone gains access to the system by hacking into it (Kierkegaard, 2011; McMullen et al., 2014; Harman et al., 2012; Rahman and Kreider, 2012; Raposo, 2015) by for example sending phishing mails to users (Kierkegaard, 2011). Other ways in which unauthorized users may gain access to the system is by password stealing, attacking the system by using software installed on a user-computer or attacking the system from the internet (Ángel DÍaz De León Guillén et al., 2020). They may also damage the system by accessing the physical servers (McMullen et al., 2014). Once they have access to the system, hackers may steal and possibly release confidential (patient health) information (Kierkegaard, 2011; McMullen et al., 2014; Harman et al., 2012; Rahman and Kreider, 2012; Raposo, 2015), causing a data leak. Hackers could also change data in the system (Schiza et al., 2016). It is therefore important that hospitals implement measures to detect, prevent and protect their EHR system.

Finally, there are security protocols and procedures. The hospital should have clearly defined security policies, and these should be followed by all staff members (Hoerbst and Ammenwerth, 2010; Rahman and Kreider, 2012; Kierkegaard, 2011). The security measures should also be standardized, for example all laptops should be encrypted . Security policies should further include protocols regarding the safe transfer of data. In order to determine whether a security breach has taken place, regular checks should be performed to identify incidents and system and process flaws. For this purpose, the EHR software should also be properly maintained. Once an incident does take place, the hospital should be able to response and recover quickly .

Content

The final risk category related to the use of Electronic Health Records concerns the data (i.e. the content) in the system, meaning the medical records among other things. Data should be properly stored and preserved to prevent data loss, and it should be available when hospital staff needs it (Hoerbst and Ammenwerth, 2010; Kierkegaard, 2011). If medical records are not available it can prevent patient care, which was the case in a hospital in Maastricht. The hospital had to cancel the treatment of thousands of patients after a computer malfunction caused patient data to be inaccessible and made the hospital unreachable digitally and by phone for 8 hours (Verkerk, 2022). The Queensway Carleton Hospital also had to deal with an offline system when a hardware failure caused not only patient data to be unavailable for 20 hours, but also the equipment to become inoperable and work phones to stop working. This led to privacy regulations being violated as doctors requested patient data, such as CT scans, using their personal cellular phone coverage. The hardware failure also caused bed alarms to stop working, due to which nurses had to check each patient every 15 minutes to see if they were okay (Anad and Chin, 2022).

The prevention or serious obstruction of patient care that the unavailability of medical records can cause can therefore endanger patients as well as cause violations of privacy regulations. Research done by Samy et al. (2010) supports this as they concluded that power failure and power loss are the greatest threat category to a hospital information system. Another threat category identified by Samy et al. (2010) is software errors. Software errors can happen when deleted data is still available in the system or records are not instantly updated (Hoerbst and Ammenwerth, 2010; Raposo, 2015). Medical records should always be up-to-date to prevent medical errors, such as the wrong medicine or medicine quantity being ordered. Furthermore, medical staff may also make errors when entering data into the system. For example, copy pasting information from one medical record to another if two patients have the same diagnosis. This becomes a risk as there may be a fault in the original text, and this fault will then be present in the medical records of multiple patients (Raposo, 2015). There may also be a mismatch between the functionality of the system and the demands of the medical staff, which may result in the EHR system fostering errors instead of reducing them (Ash et al., 2004). These errors in medical records become increasingly worrisome when professionals fully trust the system and do not question the information or the decisions that the system presents them.

In this subsection, the risks of an EHR system have been discussed. To structure the risks, they were split in 4 categories: integrity, confidentiality, data security and content. In Table 6 all the risks discussed in this subsection can be found.

Table 6: EHR system risks

EHR System risks
Integrity
Unauthorized parties read data
Unauthorized parties adjust data
There is no or an incomplete audit log
System makes changes to the data
Confidentiality
Access control is not role-based
It is unknown which users have additional privileges
User accounts are not linked to hospital staff members
No secure data transport protocol
Data security
Insider curiosity from employees or third parties
Insider subornation from employees or third parties
Human error
Hackers
Phishing mails
Accessing physical servers
No or not all security measures are standardized
Security policy is not clearly defined
Security policy is not followed
No response and recovery procedure
EHR software is not properly maintained
Content
Data is not available
Data loss (data is not stored and preserved properly)
Deleted data is still available in the system
Medical records are not up-to-date
Human errors when entering data into the system
EHR system fostering errors

3.3 Risk Management

3.3.1 Overview

Having discussed the risks of a hospital's legacy information system, it is also important to know how to handle these identified risks. For this, risk management methods can be used. The goal of such a method is to minimize the probability and impact of potential risks while at the same time maximizing these for potential opportunities (Tesch et al., 2007). To develop an understanding of risk management methods currently used, research into these methods was performed. One of the leading articles in software risk management is that of Boehm (1991). In the article Boehm describes that risk management consists of 2 steps, namely risk assessment and risk control. This research focuses on the identification of risks and determining their impact, wherefore only the first step - the risk assessment step - will be further elaborated. The risk assessment step has 3 subsidiary steps:

- *Risk identification*: produces a list of risks. This can be done using checklists or

comparing experiences for example.

- *Risk analysis*: establish the loss probability and magnitude of each risk. The loss probability is the likelihood that the risk will happen, and the magnitude is the impact that the risk has if it were to happen. Methods that can be used for this include cost models, decision analysis and performance models.
- *Risk prioritization*: rank risk using techniques such as risk-exposure analysis or risk-reduction leverage analysis.

Other methodologies use similar steps in their risk assessment, which can be viewed in Table 7.

Table 7: Risk assessment steps in literature

	Anthony et al. (2016)	Boehm (1991)	Fairley (1994)	Tohidi (2011)	Stoneburner et al. (2002)
Identification	✓	✓	✓	✓	✓
Analysis	✓	✓	✓	✓	✓
Prioritization	✓	✓		✓	✓
Includes more detailed steps				✓	✓

Although Fairley (1994) does include a probability and impact estimation for each risk, they do not mention prioritizing risks. In the methods of Tohidi (2011) and Stoneburner et al. (2002) this is also not explicitly mentioned. However, they have a specific step for risk determination, which combines the probability and impact values into a risk value. This makes it easy to determine what risk(s) should get the highest priority, and due to this reason their methods are included as having a prioritization step. Their methods also go into more detail, and have split the three steps proposed by Boehm into 9 separate steps. Both methods have the same steps, which are:

1. **System characterization**: define the scope of the risk assessment and gather information about the system.
2. **Identify threats**: threats exploit or trigger a vulnerability. Examples of threats are floods, hackers and power-failure.
3. **Identify vulnerabilities**: these are weaknesses or flaws in a system, for example a terminated employee that still has access rights to the system.
4. **Analyse controls**: determine which measures have already been taken by the organisation to prevent or minimize a threat.
5. **Determine likelihood of risk**: establish the probability that a vulnerability will be exploited, then rate this probability as high, medium or low.
6. **Analyse impact**: analyse what impact the risk will have on the integrity, availability and confidentiality of the system. Determine if this is high, medium or low.
7. **Risk determination**: assess the level of risk. That can be done using one or a combination of the likelihood of the risk, impact of the risk and/or adequacy of the controls. It can be useful to make a risk-level matrix that includes the likelihood and impact of the risk.

8. **Control recommendations**: establish which measures could prevent or minimize a risk.

9. **Document results**: provide documentation (for example a report) of the results of the risk assessment. This can help managers become aware of the risks as well as take the risks into account when making decisions about the system.

This approach gives a clearer overview of what a risk assessment team should do and provides them with more structure. This would be beneficial to a team that does not or have minimum experience in performing a risk assessment. However, the use of any of these methodologies has several success factors and shortcomings that should be taken into account when using them. These will be discussed in the next subsections.

3.3.2 Success factors

For a successful execution of a risk assessment several actions have been identified by researchers as beneficial. Stoneburner et al. (2002) mentions the importance of senior management's commitment, and Tohidi (2011) even proposes a top management committee to be assigned to the risk assessment. This is important as they can provide the resources to perform the risk assessment as well as adjust decision-making processes to incorporate a risk mitigation strategy. The management can also make system users aware of the risks as well as the preventive measures that may have resulted from the assessment. Additionally, the researchers stress the importance of the full support and participation of the IT department(s), as well as having a qualified team to do the risk assessment. Next to that, Heemstra and Kusters (1996) mention the advantage of having a neutral party lead discussions during the risk assessment. This can improve discussions as the neutral party, unlike the employees of the organisation, does not have stakes in the risk assessment and their only goal is to have an accurate risk assessment. Tohidi (2011) further states that in these discussions, specifically when estimating and evaluating risks, the organisation's mission should be taken into account. This ensures that relevant risks are selected and given the proper priority. Something that can help determining the risks is the use of a checklist, although this checklist should not contain more than 36 items (Heemstra and Kusters, 1996). Finally, Taylor et al. (2012) recommends using graphs for communication to all stakeholders as it allows them to understand and discuss the risk assessment better.

3.3.3 Shortcomings

The risk management methodologies mentioned have several shortcomings, which can be categorized into three categories: 1) problems and oversights of the methodologies; 2) problems with executing a risk assessment; and 3) issues in the way that managers handle the results of the risk assessment. Starting with the problems and oversights of the methodologies, many approaches (such as Boehm (1991) and Fairley (1994)) use risk probability and impact calculations. These two estimates are however hard to accurately predict, especially as not all information about the system and its users is available in most cases. Consequently, when one or both of the estimates are assigned a value, this value is considered to represent a stronger knowledge than is justified (Aven, 2016). Because it is difficult to estimate the risk probability and impact of a risk, methodologies use the assumption that managers have adequate knowledge to calculate them, which is often not the case (Taylor et al., 2012). Next to that, risk management methodologies have a standardised format, which can make it difficult to apply to different circumstances (Lyytinen

et al., 1998). They are also often presented in blocks of text with very little visual representations. This form of presentation is meant for communication to other academics and not managers, and makes it difficult for managers to easily understand and use the risk management methodologies (Taylor et al., 2012). Additionally, many methodologies do not provide collaborative support to the risk assessment team, or promote interactions with users that are spread across different geographical regions (Anthony et al., 2016). Furthermore, Lyytinen et al. (1998) states that most risk assessment methodologies disregard the possible positive outcomes that can result from a risk being avoided, and instead only focus on negative outcomes and how to avoid them.

Next, there are several problems when executing a risk assessment. Firstly, project managers have limited time and resources available for the risk assessment (Taylor et al., 2012). This may result in the risk assessment not being finished, or the risk assessment team rushing the assessment and missing important risks. In their research Taylor et al. (2012) also found that, in many cases, only the risk identification stage is completed. This is a problem as, if the risks are not further researched, managers may perceive certain risks as having a higher impact and/or probability than warranted, and handle in a way which will cause more risks or cause other risks to become a reality. Moreover, Taylor et al. (2012) observed that only completing the risk identification stage happened more often when using a checklist as opposed to other risk identification methods. Another risk of using a checklist, is that it is often assumed that the checklist is complete, and risks that are not mentioned on the checklist are overlooked (Heemstra and Kusters, 1996; Taylor et al., 2012).

Finally, managers may not be able to handle the results of the risk assessment adequately. They are likely to be insensitive to the risk probability estimate, and will instead focus on the possible impact of the risk. This causes risks with a high probability of occurring to be overlooked as well as the extent to which a risk can be controlled (Lyytinen et al., 1998; Taylor et al., 2012). Next to that, managers tend to make fast decisions or delay decisions to avoid a risk, which may both result in the risk occurring (Lyytinen et al., 1998). As the methodologies do not take this illogical behaviour into account, this is also a shortcoming.

3.4 Conclusion

This literature research gives an insight into which risks a hospital's legacy information system presents. To determine the most important risks, a table was made with the risks that have been mentioned in two or more papers. This overview is in Table 8 on page 26, and includes the number of papers in which each risk has been mentioned. The risk that is mentioned the most overall is that a legacy system is hard to modify, which will result in the system not meeting the functional and security requirements of the hospital. The most mentioned risk regarding the use of COTS software is that the source code is unavailable to the hospitals, making them dependent on the provider for maintenance and updates. For the risks that hospital circumstances present, there is no single risk that is mentioned most. However, each of the risks mentioned in multiple papers results in healthcare being obstructed or, in the worst case, inaccessible. This literature study also researched different risk management methods, and found that the method proposed by Boehm (1991) is the most influential. This method has 3 steps for risk assessment: 1)

risk identification, 2) risk analysis and 3) risk prioritization. The other methods found included these steps, with the methods proposed by Stoneburner et al. (2002) and Tohidi (2011) having more detailed steps. Their methods, which includes 9 steps, describes the steps for identifying risks, assigning a probability value and determining the impact in more detail, which provides more guidance to a risk assessment team. It would therefore be best to use one of their methods for a risk assessment of a hospital legacy information system.

Table 8: Hospital legacy information system risks that have been mentioned in 2 or more articles. The # column is the number of articles that mentioned the risk.

Legacy system risks	#	**COTS software risks**	#
Hard to modify	5	Black-box	3
Finding experts to maintain the system is difficult and expensive	3	Dependence on provider for maintenance	2
Lacking documentation	3	Undesirable/dangerous effects with update	2
Competitive disadvantage compared to new(er) technologies	3	Safety implications of the software and/or it's updates are not clear	2
Maintenance is time consuming	3		
Maintenance is difficult	2		

Hospital specific risks	#
Power failure/loss	2
Technological obsolescence	2
Hardware failures	2
Software failures	2

Chapter 4

Results

In this chapter the risks that were given during the interviews will be discussed according to the KPMG categories. For each category, the risks that were either discussed extensively or mentioned by multiple participants will be discussed in detail. The description of the risks will focus on explaining how risks can manifest and what measures hospitals take to prevent the risk. Quotes from the participants will be given to support the statements that they made. To create a full overview of all the risks that were found in the interview, the final section will shortly discuss the other risks that were determined during the interviews - meaning the risks that were not discussed extensively or mentioned by multiple participants.

In total 29 risks were found during the interviews, which are stated in Table 9. In the table, it is also stated which participant mentioned risks in which category. In order to protect the anonymity of the participants, it is not mentioned which participant(s) mentioned which risk. Furthermore, all participants worked at a hospital that has the Electronic Health Records system Epic when the interviews were conducted. The risks found therefore apply to this system.

4.1 General Information Security

This category describes risks related to the vision and policies of the hospital. During one of the interviews the risk of data inaccuracy - otherwise known as the integrity of the data - was discussed extensively. Two ways in which this risk manifests were specified. Firstly, when staff members accidentally put patient data in the wrong medical record, and secondly when any information has to be handled manually, outside of the system. Examples of when data inaccuracies can happen is when a document is named incorrectly, for instance with the wrong patient name. It can also happen that a staff member makes notes about a patient in the wrong medical record (i.e. the medical record of another patient), which is often discovered as the notes differ from the treatment that the patient is receiving. Inaccuracies are also likely to occur when faxing patient information. This information is copied by hand, which is error sensitive. The social security number of a patient, for example, can easily be copied incorrectly when done manually. Staff putting information in the wrong record is most likely to happen with twins. The information that staff use to identify a patient is mostly - if not fully - the same with twins. P1 explained:

"What does happen is in a medical record of a twin, where both are 19 years old and live

Table 9: The risks that were identified during the interviews per category. The X's mean that a participant discussed risks within the category.

	P1	P2	P3	P4	P5
General Information Security	**X**				
Data is inaccurate (integrity)					
Shadow IT					
IT department is underfunded and overworked					
Access to programs and data	**X**			**X**	**X**
Unjustified access to a medical record					
Access policy is not adhered by staff					
Unauthorized access to programs by users					
Ill-intentioned staff member					
Accounts that are not linked to a staff member					
Continuity	**X**	**X**	**X**		**X**
Availability of the system and the medical records					
Power failure					
Network is unavailable					
Cyber security	**X**		**X**	**X**	
Old hardware					
Patient information is saved outside of Epic					
Security of the patient portal					
Data breach by unauthorized user					
Cyber security attack					
Change management		**X**		**X**	**X**
Releases/updates can not go live					
Changes have unexpected impact					
Black box					
Old base of the system					
Large size of the system					
Missing overview of the full system					
Dependence on expert opinions					
Upgrades from Epic that may cause a crash					
Supplier management		**X**		**X**	
Different laws and regulations in the United States and the Netherlands					
Epic is expensive					
Bugs in the system					
Third party management					
Trustworthiness of Epic					

at the same address, have the same birth date and for one reason or another parents like to give both of them a name with the same initial. That's where things sometimes go wrong."

One of the consequences of inaccurate data is that the hospital has to report these to the Dutch DPA (Autoriteit Persoonsgegevens), which is an independent regulator that is concerned with the protection of personal data (Autoriteit Persoonsgegevens, nd). There may also be damage to the reputation of the hospital. In the worst case an operation is done incorrectly, such as that the left leg is amputated instead of the right leg. However, the participant that gave this example explained that this type of incident is extremely unlikely as both patients would need to have problems with one of their legs. Nonetheless, to prevent data inaccuracies from happening all data mutations made in the system are recorded. Prevention is also already in place during the treatment of the patient, as their data is viewed by many different people such as the doctor, nurse and receptionist. This makes it likely that the staff will notice and correct any inconsistencies. However, if it is not noticed, it will be recognized during invoicing, as the medical record of the patient has to be checked in order to send the invoice.

Another risk of general information security is the risk of having shadow IT in place. Shadow IT are programs that have not been developed nor approved by the IT department, but which the hospital staff uses for their work nonetheless. No data and privacy impact assessment, nor a security assessment has been carried out on these programs. Patient data may be stored in them, meaning it is stored outside of the hospital environment and the hospital may be liable for noncompliance with security requirements. Moreover, as it is not regulated by the IT department former staff members may still have access to these programs, and therefore to confidential information. The reason these programs are used is that it may take months for the hospital's IT department to implement a feature that they request, due to the IT department having a high occupancy rate. Therefore, instead of waiting they use shadow IT. The participant explained that, when the hospital discovers the use of shadow IT, they do not instantly prohibit the department from using it. P1 stated:

"It's not so much that I don't want people to use the application (shadow IT), but if it's getting used, then it needs to comply with a number of requirements to cover the risks."

The hospital will assess if the programs comply with their data, privacy and security standards. To gain awareness of the use of shadow IT, staff is also requested to report any shadow IT they may use to the IT department so it can undergo an assessment. However, this assessment is more work for the IT department which further increases their occupancy rate, delays projects, and increases the waiting time for new projects.

4.2 Access to Programs and Data

"I think that access to the medical record is our biggest risk. Regarding the access to programs and data and general information security categories."

In this category, P1 stated that unjustified access to a medical record was the highest priority risk. Moreover, another participant addressed this risk as well. Unjustified access to a medical record is when an authorized user of the system accesses the medical record

Table 10: General Information Security Risks.

Risk	Manifestation	Prevention
Data inaccuracy	Patient data is put in the wrong medical record	1) All data mutations are recorded in the system; 2) Patient data is viewed by many different staff members which often catches a mistake
	Information is processed manually	Try to limit the amount of data processed manually
Shadow IT	Departments don't want to wait for months to be able to use a feature they request	Staff members are requested to report the use of shadow IT

of a patient unwarranted. To prevent this there is a break-the-glass procedure, which takes place when hospital staff tries to access a medical record of a patient with which they do not have a treatment relationship. This procedure requires the staff member to give the reason that they are accessing the record, which is saved in the system. After filling it in, the staff member will receive immediate access to the record. Immediate access is important as a patient may need urgent treatment, for example if they are at the emergency care department. P1 stated:

"A treatment relationship is very volatile. It is something that may exist in reality, but which cannot be represented in the system yet. It is the chicken-egg story of course. Which came first, accessing the medical record or the treatment relationship?"

Nonetheless, immediate access can cause problems, as was the case when Barbie was hospitalized in the hospital. As mentioned in subsection 3.2.3, hospital staff accessed her medical record unjustified, resulting in disciplinary actions against the staff members and a 350,000 euro fine for the Haga hospital (NOS Nieuws, 2018, 2019; RTL Nieuws, 2018).

However, unjustified access can also take place without triggering the break-the-glass procedure. If a patient is hospitalized, all nurses in the department they are hospitalized at will have a treatment relationship with them in the system, and therefore access to their record without a break-the-glass procedure. Yet not every nurse will actually treat the patient. Nurses are assigned to certain beds in the department, for example one nurse may treat the patients in beds one to four, another the patients in bed five to eight, et cetera. Therefore, a nurse can access a medical record of a patient they are not treating unjustified and without going through the break-the-glass procedure. These types of accesses to medical records are hard to monitor, as a hospital has thousands of accesses to medical records per day. Hospitals therefore rely on spreading awareness about the access policy in hopes to prevent it. They will inform staff of what is and is not allowed, and also question staff members when they suspect a medical record was accessed unjustified. Nonetheless, it takes time to examine whether access was justified, and it therefore costs a lot of resources. P1 elaborated:

"We have thousands of cases where someone opens a record per day. And that has to be checked. Yeah, how are you going to check that? Because you're not going to check for each one of them if the medical record access was justified or unjustified."

There is also a lack of testable hypotheses which would make it possible to automate (part of) the access policy monitoring, though a participant stated that several hospitals are

developing these. Unjustified access may therefore still take place and even go unnoticed. Hospitals do have several random sample tests to monitor the access policies, as well as separate random sample tests among users with extensive privileges. They also have general checks for patients and hospital staff with the same last name to try and find family members, as there is a higher probability that hospital staff will try and access the medical record of a family member. Yet, the most common case of unjustified access is a hospital staff member accessing their own record through the system instead of through the patient portal, which is prohibited as a patient is not allowed to view all the information that is gathered about them (for example the doctor notes).

When discussing the risks, a difference should be made between unjustified access to medical records and unauthorized access to Epic. Unauthorized access can take place when a former employee still has access to the system or access privileges are assigned to the wrong user. For instance, someone from the administration team receives the role - and therefore access privileges - of a doctor. They will then be able to register a consult with a patient in the system despite it not taking place, which will then be invoiced to the health insurance of the patient. This is not just problematic as it is fraud, but it also violates the privacy of the patient. Alternatively, unauthorized access can also take place with users that have extensive privileges and misuse them, which the participants stated as a particularly important aspect of this risk. P5 stated:

"We monitor the on-call accounts extensively as it is an account that could be misused. That is a risk."

Examples of users with extensive privileges are administrative, accessibility and on-call users. Someone with an administrative role could, for example, commit identity theft by overwriting the access security and then using the account of another staff member. Special attention is paid to these accounts in order to ensure that they are not misused. The monitoring of the accounts includes examining the account activity and verifying regularly whether the staff members linked to these accounts are still employed at the hospital and still employed in a job function which requires the user to have access to an administrative role. A complicating factor to the monitoring is, however, that multiple staff members may have access to such an account. In other words, some of the accounts may be shared between staff members and are not linked to a single staff member. It then becomes unclear who used the account, and extra supervision is necessary. For such cases, it should be thoroughly monitored who is using the account, at which day and what time, preferably with their work schedule to confirm their use of the account.

Another risk mentioned is the risk that staff members do not adhere the access policy. This often happens when a staff member does not yet have the correct privileges for their role, for example when they switch departments. Interns (called 'coschappen' in Dutch) have to work at different departments during their internship, they may not have access to the documents they need in the first few days in a new department. In order to still acquire the information they need, a doctor at the department may open the documents on their account for the intern to look at. This is against the access policy of the hospital. New staff members are also likely to not have access to the system yet. They need to complete an Epic training before being granted access to the system, and their manager has to request both access privileges for the staff member as well as register them for this training. If managers forget to do this, the new staff member will not have access to the

Table 11: Access to programs and data risk.

Risk	**Manifestation**	**Prevention**
Unjustified access to medical record	Staff member accesses a medical record of a patient they do not have a treatment relationship with	Break-the-glass-procedure
	Staff member accesses a medical record of a patient they do have a treatment relationship with but are not treating	Spreading awareness of the access policy; spreading awareness that the access policies are being monitored; random sample testing of accesses; checking if last names of staff members are the same as patients
	Staff member looks at their own medical record in the system	
Unauthorized access to Epic	Former employee still has access to the system	Regular checks of which employees left the hospital and if they still have access to the system
	Privileges are assigned to the wrong user	Regular checks of access privileges
	Misuse of access privileges by users with extensive privileges	Closely monitoring the account activity of user accounts with extensive privileges
Staff members do not adhere the access policy	Staff member does not yet have the privileges they need for their role	Open discussions with the hospital departments to find solutions for prevention; break the glass procedure
Ill-intentioned staff members	Staff members put malware or ransomware on the system or otherwise damage it	Extensive security measures on the hospital network
	Staff members with extensive privileges put malware or ransomware on the system or otherwise damage it	Extensive security measures on the hospital network
	Insider subornation	Only reporting user accounts can export large files from Epic

system for one or more days. They may then use the account of a coworker to access the system, which again is not allowed. Other examples in which the access policy may not be adhered are with staff members that do not work at the hospital full-time, for example someone that comes once a month to conduct checks or a freelancer, and staff members that support multiple specialists which makes their role hard to define in the system. To ensure that access policies are followed, the IT department will have open discussions with the hospital departments to discuss what is possible to prevent it. They will also spread awareness among the managers and inform them that they have to request access privileges and register new employees for an Epic training on time. The break-the-glass procedure also serves as means to enforce the access policy. Finally, one of the participants also said that they have accepted that this risk will happen, and they cannot prevent it completely. The impact of this risk, however, can be substantial. P4 stated:

"Do we know the impact of it? Maybe it's not big short term, anyway. Of course, if later it turns out that something is wrong medically, then there is a bigger impact."

If a medical error is made, it may not be traceable in the system whom made the decision that led to the error. This may happen in a surgery room, where a separate computer for each staff member participating in the surgery is not available. One of the staff members will then log into a computer, which their coworkers will proceed to use as well. As it is too much effort and too time consuming to log out and back in every time that another person uses the computer during the surgery, all the information about that surgery will likely be registered on a single staff member. To prevent the risk, participants mentioned that they should be able to speed-up the process of giving a staff member access privileges, such that it can be done on the day they are requested. They also mentioned that managers should be trained better such that they know the procedure for new staff members. Finally, it should be mentioned that this risk causes other risks for the hospital. First of all, the compliance of the hospital will be compromised, and secondly it causes their logging to be incorrect. The latter can cause medical errors to be untraceable, as was mentioned above.

The final risk that will be discussed of this category is that of ill-intentioned staff members. Ill-intentioned staff members may put malware on the network, intentionally damage the system, or intentionally delete data. This risk more significant with users that have extensive privileges, as it is easier for them to do as well as harder for the hospital to detect. The possibility of ransomware, which encrypts data and makes it unreadable, is especially concerning to hospitals as it will make patient data unavailable and hinder their ability to provide care. Next to that, an ill-intentioned staff member can threaten the confidentiality of patient data by sharing information with outsiders. Parties that would be interested in this information are - according to the participants - not only criminal organizations, but also the Chinese and Russian governments. It is possible that these parties either try to get a spy to work in the hospital, or try to convince a staff member to work for them. Ill-intentioned staff members can cause a data breach and compromise the integrity and availability of the system. To prevent it hospitals have taken extensive security measures on their network, often working with multiple parties to monitor their network. Next to that, Epic has taken measures that make it more difficult for staff members to export large amounts of information out of Epic, which also makes it more challenging to share large amounts of information with outsiders. Epic has done this by developing a special role, and only staff members with this role can export large files from the system.

4.3 Continuity

On the question if any of the risks were more important than others, P2 answered:

"Continuity I think. I think continuity is a risk that touches everything, so continuity."

In this category, the availability of the system (and therefore the data) was mentioned by three different participants as a risks, with P2 stating it was one of the highest risks of Epic. A hospital uses a variety of software which are linked with each other, if one of these gives an error it may cause a chain reaction and result in an error in Epic and Epic being unavailable. It may also happen that certain parts of Epic are unavailable, such as the video call with patients functionality, or the patient portal. According to P2:

"Many components are needed to make the EHR available to healthcare providers and patients. [...] There is a lot in the chain of components. There is still a risk there, the chain dependency is just very big"

Epic is also offline during upgrades, which are often done in the evening and night in order to minimize the hindrance to the provision of care. However, the upgrades become problematic if they take longer than planned, for example if they have to start later as operations extend past the normal times. The system may then be unavailable during the opening hours of the hospital. Other ways in which the risk can take place is by the use of outdated IT. For example, the computers that end users use for work (for example the nurses) may be running on an old Windows version. Epic becoming offline can have major impact on the hospital. In the worst case, they have to send patients home, stop or delay operations and cancel appointments. Moreover, it will cost the hospital money as they cannot treat patients. P3 stated:

"There are people that think we (the app) can easily go without the app for a day. I think that if it's not available for 20 minutes, we're going to have to send people home. And that costs money."

Extensive measures have therefore been taken to ensure it does not happen, such as regular testing of the power supply and network of Epic. Most hospitals also have a copy of Epic in a data center, and they may have computers with a separate power supply that can be used in case there is a power failure. Other parts of Epic, and that are important for the use of Epic, have also been made redundant, such as having multiple internet connections and maintaining several backups instead of one. However, P3 mentioned that there is a downside to investing so many resources into ensuring the availability of the system:

"We have little to no experience with the system being unavailable, which also doesn't help with creating awareness among end users. Especially about the fact that it can happen. Then they (the end users) say "Yes, but I've been working here for 5 years and it never happened." So that is a disadvantage of setting things up too well, isn't it?"

In other words, because the system is never offline hospital staff is not prepared for when it does happen. They do not inform themselves on what options are available to still access medical records if the system is offline as they trust the system to stay available. Another way in which the system can be made offline, is by hackers. This will be discussed more in section 4.5.

Table 12: Continuity risk.

Risk	Manifestation	Prevention
Availability of the system and the medical records	Epic has a chain dependency on other software	
	Epic is offline during upgrades Use of outdated IT	Schedule updates outside of the hospital working hours General prevention measures: parts of the system are redundant; regularly making back-ups of the system
Power failure		Regular testing of the power supply
Network is unavailable		Regular testing of the network; multiple network connections

4.4 Change Management

Change management focuses on which modifications to the system are made, when and how. It concerns any protocols that are in place regarding changing the system as well as how to evaluate the impact of changes to the system. In the previous section the risk of Epic being offline was discussed. However, parts of Epic may also become unavailable due to a change having unexpected impact. The risk of changes having unforeseen impacts is, according to P4, the biggest risk within change management. When asked what the biggest risk within change management is P4 answered:

"We have noticed that the production of changes to Epic has unexpected impact and this has various reasons. Sometimes a bad judgment is made, where they (hospital staff implementing changes in Epic) didn't know all the places where a certain change would impact."

They specified the biggest risk to be the changes that the hospital themselves makes, as opposed to upgrades provided by Epic. Unanticipated impacts can happen due to a number of reasons, among which are: the impact of the change was misjudged, there is not enough knowledge available to judge the impact of a change, and changes have been insufficiently tested. Additionally, often departments can change the parts of Epic that they work with independently of the IT department, which may result in modifications being tracked in different tools. This will result in a loss of overview and control of the changes that are made, reinforcing the lack of knowledge to judge the impact of a modification. Teams may further choose to ignore change protocols and implement their own vision on how to make changes, which also increases the risk of modifications having an unforeseen impact. Other factors that contribute to this risk, is that the system is large and complex, making it hard to predict the impact of the change. Upgrades provided by Epic may also cause an error, as Epic is highly customizable for each hospital. When a hospital chooses to use Epic, each start with the same (basic) version of Epic. However, they can - and do - customize the system to such an extent that they create a unique

version of Epic, which results in every hospital having a unique and different Epic version. An upgrade of Epic may therefore not be compatible with their version of Epic. However, Epic pays a lot of attention to their upgrades, and therefore the participants do not think it is likely that the upgrades will have any major unforeseen impacts on the system. The changes made by the hospital form the biggest risk. These changes may be adding a new medication, dosage, or way to take to medicine to the medication list, or changing forms. Some examples mentioned of unforeseen impacts are that users with a specific role cannot see a button or that a functionality is temporarily disabled as the modifier did not notice that it was set to disabled when they made the change live. To prevent this, hospitals raise awareness of issues that can happen with developers. P2 stated:

"You always have risks, it is of course an Electronic Health Record. That is also the mindset that we constantly use: know what you're changing, and validate it in multiple test environments."

Hospitals have several test and control procedures in place before a change is live, as well as a progress for requesting changes. As unforeseen changes can compromise or even obstruct patient care, and threaten the integrity of the system, they also have a procedure in place that allows them to quickly respond if a change does have an unexpected impact.

What contributes to the previous risk, is that hospitals often lack a complete overview of the system. Due to the customizability of Epic, it can be difficult to keep track of all the changes. As mentioned, each department can make changes to the modules they work with to fit their needs. However, due to this large amount of people working on the system, documentation of modifications made may not be done well. This results in a number of issues. First, it is difficult to gather a clear overview of all the modifications that are made, and therefore the IT department does not have a clear overview of how the system works and which features are activated and used. Second, it is labor-intensive to check all the changes and verify if they will work correctly. Third, the quality of the system may be degraded due to the many modifications made to it. Moreover, due to Epic being highly customized to each hospital, it becomes difficult for hospitals to share their features with each other or implement a feature together. The hospitals thus have to invest more time, costs and resources than if they could build features together.

4.5 Cyber Security

A successful cyber security attack can impact the integrity, confidentiality and availability of Epic. P3 stated:

"It will cause other risk if it (the attack) compromises the integrity of the system. Then you get risks on things like the patient data. But well, that won't happen anytime soon. I'm saying that, but of course it's always possible."

Several ways in which a hacker can gain access to Epic through the users were specified by the participants. Firstly by password hacking, where a hacker uses the credentials of a user in order to access the system. It can also be due to mistakes or negligence of the staff, such as leaving devices unlocked, or not using two-factor identification. However, even with two-factor authentication a hacker could gain access to the system using user credentials. Once they have the credentials, they may spam the user with requests to log

Table 13: Change Management risks.

Risk	**Manifestation**	**Prevention**
A change that the hospital makes to the system has an unexpected impact	Impact of a change is misjudged	Raising awareness; Test and control procedures
	Lacking knowledge about the system	
	Change has not been sufficiently tested	
	Loss of overview of the full system	
	Epic is a large and complex system	
Upgrade of Epic has an unexpected impact	Due to the high customizability of Epic, every hospital has their own version of Epic	Epic takes the different versions into account and offers support
Lacking a full overview of the system	Lacking documentation of the system	Raising awareness
	Departments can make small changes to the system themselves	

Table 14: Cyber Security risks.

Risk	**Manifestation**	**Prevention**
Hacker gains access to Epic	Password hacking	Two-factor authentication; monitoring the accesses to Epic; awareness campaigns for staff; ethical hackers; application for exchanging data with other software; special measures if a third party requires access to Epic
	Staff negligence	
	Staff download a corrupt file or program	
	Staff and patients entering the system from their home network	
Malware	Hacker gains access to Epic	Next to the previously mentioned preventive measures, back-ups and the regular testing of back-ups
Ransomware	Hacker gains access to Epic	

in. If the user only has to confirm that they are trying to log in they may give in and confirm in order to make the continuous requests stop, giving the hacker access to the system. To counter this, hospitals can use a different two-factor authentication method with which the user has to fill in the number that is displayed on the screen in which the log-in is taking place. However, hackers can also manage to gain access to the system when a staff member accidentally downloads files on their device that are corrupted by the hacker. A staff member may download files or other programs on their device for personal use, and they may save confidential in those programs. For example a Word document that they use. If staff members work from home, or at the home of a patient, they are likely to also access the system from that network, which may be unsecured. This gives another opportunity for hackers to enter the system. Hospitals have taken measures to prevent hackers from gaining access to their system. They keep track of all accesses to their data, have awareness campaigns for employees as well as a hotline for data breaches and have software that constantly tries to detect data leaks. They may also use ethical hackers to try and find weak points in their security. Next to that, hospitals are developing an application to exchange data from Epic with other software, creating safe method to transport data. Special measures, such as an Epic read-only version, may be taken with the parts of the system that are shared with third parties.

Another approach that hackers can use is trying to install malware in the system. P3 found this the biggest risk regarding cyber security, especially as it can be in the hospital's network before it activates and encrypts data in the system. P3 explained:

"If they manage to encrypt your data, then you have a problem. Also because of the size of the system, you don't have a backup of all the data."

Hackers can also use ransomware to threaten the hospital, which P1 and P4 found the highest priority risk of cyber security. When asked what were the greatest risks, P1

elaborated on cyber security:

"If you really look at cyber security, then you're of course going to talk about the ransomware that affects the availability. And integrity and confidentiality are the biggest risk that we have in the cybersecurity domain."

Next to the measures stated in the previous paragraph, hospitals can make a backup of their system and the data to ensure that data is available at all times. These back-ups should also be regularly tested to ensure that they work.

4.6 Supplier Management

The final risk category is supplier management. The risk named immediately by participants when discussing this risk, is the fact that Epic is an American company. It therefore operates with different laws and regulations than the Netherlands. This can result in Epic offering a functionality that is not allowed in the Netherlands, such as certain information being visible to the patient (in the patient portal) which they are not allowed to see according to Dutch laws. It may also be the case that Dutch laws require extra information or security measures whereas this is not required in the United States. For example, to use the DigiD, which is a unique log-in that for Dutch citizens and is linked to their social security number (DigiD, nd), the Dutch government requires strict security measures. Hospitals therefore need to request adjustments to the system in order to be able to use DigiD. This results in extra work for the hospitals, as they have to ensure that each upgrade complies with the Dutch laws, as well as possibly extra costs from Epic in order to adjust the software. They therefore need to make a consideration each time between paying extra costs and how to fully comply with Dutch regulations. It can be the case that a functionality added by Epic is not available in a hospital, as a hospital does not consider it beneficial to pay the costs in order to make the feature compliant with Dutch laws and therefore disables it. In the worst-case scenario, an update will have to be postponed in order to make it compliant. Other problems may arise as Epic and the Dutch hospitals can have different insights and priorities, as well as Epic not being allowed to access all the data of Dutch hospitals by law. P2 elaborated:

"Epic gathers a lot of data about how we use our Electronic Health Record, which they use to help us improve our Electronic Health Record. And then, of course, you get the risk of what they can access. And then you have conflicting rules regarding laws and regulations. Also there's the fact that Americans can be instructed to gather data from citizens outside of the United States."

These problems can lead to tensions both between Epic and the hospitals as well as within the hospital itself. With Epic tensions can arise if an upgrade does not comply with Dutch laws, but Epic does pressure the hospital to implement the upgrade. Within the hospital, there can be tension if hospital staff needs to work overtime in order to ensure an upgrade complies with Dutch laws and regulations. However, a participant did state that Epic is conscious and considerate about other laws. They release monthly reports that inform the hospitals' laws and regulations in the country of the hospital, and if a functionality is illegal in the country of the hospital, they will provide a workaround without charging extra costs. P2 even stated:

"They do stakeholder management very well. It is more of a risk that we as an organization sometimes can't really keep up well, right?"

Table 15: Supplier Management risk.

Risk	Manifestation	Prevention
America and the Netherlands have different laws and regulations	Epic implements a feature that is not allowed in the Netherlands	Epic keeps track of any changes in the Dutch laws and regulations; Epic accommodates changes without requiring an extra fee to make an upgrade comply with Dutch laws and regulations
	Dutch hospitals need to put in more work to make Epic comply with Dutch laws and regulations	
	Epic is not allowed to access al data from Dutch citizens	

4.7 Other risks

As mentioned at the beginning of the chapter, only risks that were discussed extensively during interviews or were mentioned by multiple participants would be discussed in detail. However, to provide a complete overview of the risks that were gathered with the interviews, the remainder of the risks will be shortly mentioned in this subsection. Firstly, regarding general information security, P1 mentioned that the IT department is underfunded and overworked, resulting in important projects being delayed and little time for new projects. As for access to programs and data, it was stated that some accounts are not linked to a single staff member. This was already briefly explained during the access to programs and data section (section 4.2), however a participant named this as a separate risk.

There were several risks in change management that have not yet been discussed, starting with the Epic releases. Epic provides new releases four times per year, which the hospital first has to test with their Epic version to ensure that the new version works and does not cause the system to crash. However, if the hospital is not able to fully test the new release they may not make their deadline to produce the new release, which is a risk. Complicating the risk, is that one of the participants described the Epic system as a black box and that the base of Epic is old, using techniques from the '70. Next to that, Epic is a large system. All these factors result in a hard-to-understand system, and the need for experts. However, hospitals have difficulty securing this knowledge and it is a risk that they depend on expert opinions in order to maintain and upgrade Epic.

Regarding cyber security, the use of old hardware - such as old laptops - is a risk. Another risk is when patient information is saved outside of Epic, for example in a Word file or on a USB, as these do not comply with the necessary security requirements. The final risk that was mentioned for cyber security is the security of the patient portal. As this is the part through which all the patients can access their medical records, it has a great risk of being hacked into.

The final category of risks that have not been discussed yet is supplier management. Risks

Table 16: Other risks.

Category	**Risks**
General Information Security	IT department is underfunded and overworked
Access to programs and data	Accounts that are not linked to a single staff member
Change Management	Releases/updates can not go live
	Black box
	Old base of system
	Large size of the system
	Dependence on expert opinions, difficulty securing knowledge
	Upgrades from Epic that may cause a crash
Cyber security	Old hardware
	Patient information is saved outside of Epic/hospital systems
	Security of the patient portal
Supplier Management	Price of Epic
	Third party management
	Bugs in the system
	Trustworthiness of Epic

that were mentioned are the trustworthiness of Epic, possible bugs in Epic and the price that Epic costs. Third-party management was also stated, as parties with which the hospitals may not fully trust Epic based on their own experiences with commercial-off-the-shelf software.

Chapter 5

Analysis

In this chapter, the results presented in chapter 4 will be compared with the findings of the systematic literature research described in chapter 3. This will be carried out by comparing the risks per category. To make the comparison, the risks that were found in literature were categorized in the KPMG categories that were used for the interviews. This categorization was carried out under the supervision of KPMG, and can be found in Appendix C. An important remark on the literature categorization is that both the author as well as KPMG were of the opinion that most risks could be sorted into multiple categories. However, this would not result in a clear overview, make the categorization repetitive, and would create the impression that literature resulted in more risks than what it actually did. Therefore, the choice was made to categorize each risk in one category only. Furthermore, any statements and risks that stood out during the interviews will be further discussed .

Table 17 is the first comparison made between the interviews and literature research. In the table the total number of risks found per research method are stated as well as the number of unique risks. Unique risks are risks that were not found by the other research method, so the risks that were found in the literature research but not mentioned by the participants and the other way around. From the table it can be observed that more risks were found with the literature research. This is because over 53 papers were analyzed for the literature research, whereas five interviews of the duration of an hour were conducted. There is therefore a difference in the quantity of information that was obtained between the two research methods. However, despite the literature research resulting in more risks, the interviews gave a more detailed description of the risks, which was not present in literature. The interviews also are also valuable as the participants are focused on real-life risks, how they work and how to prevent them, whereas literature is focused on the risks in theory. This can also explain the differences - between the risks specified in literature and in the interviews - that will be discussed in this chapter.

Looking at Table 17 again, more unique risks were found during the literature research in every category except for the change management category (in which the number of unique risks is equal). Notably, no unique risks were found during the interviews that concern continuity. Next to that, the general information security category has the most unique risks, with none of the risks found in the literature research being mentioned by the participants. It is important to note that some of the risks can be categorized in multiple categories, but have been categorized in only one category for simplicity. It is therefore

Table 17: Difference in risks found in the systematic literature research (SLR) and the interviews.

	Total number of risks		Unique risks per research method	
	SLR	Interviews	SLR	Interviews
General information security	4	3	4	2
Access to programs and data	11	5	7	1
Continuity	18	3	7	0
Change Management	5	8	1	1
Cyber Security	21	5	5	2
Supplier management	20	5	12	2
Total	*79*	*29*	*36*	*8*

possible that none of the general information security risks found in the literature research were found in the interviews, but some interview risks were found in literature. For example, data inaccuracy was mentioned by Participant 1 as a general information security risk. Part of data inaccuracy is that data is incomplete, which was sorted as a continuity risk during the literature research. This demonstrates that risks can and do overlap with multiple categories, but in order to keep the results clear each risk has been sorted into only one category.

In this chapter, the difference between the literature research and the interviews will be discussed in more detail per category. The risks of each category will be compared and differences highlighted. Next to that, the risks found in the literature as well as statements of the participants will be examined.

5.1 General Information Security

The only risk of this category that was confirmed by both research methods is that of data inaccuracy, which was already discussed above . The unique risks of this category can be viewed in Table 18. Of these risks, the risk of security policies not being followed was mentioned by two separate research articles, but not by any participants. A reason for this is can be that the hospitals have an explicitly defined security policy. It is therefore likely that they have a security policy, as well as standardized security measures. As for the unique risk of not having any data transfer policies, one of the participants stated that they are working on a software with which they can safely transfer data from Epic to other software. It is thus still a risk, but prevention measures are being taken. The final unique risk of the literature research, the lack of a legal framework for liability issues, will be discussed together with the unique risk of shadow IT. Participant 1, who mentioned the risk, stated that they do not object to the usage of shadow IT but that it does have to comply with the security requirements. However, the usage of shadow IT can violate the GDPR regulations - especially if patient data is saved on it - and may result in a fine up to 4% of the annual turnover of the hospital (European Parliament and Council of the European Union, 2016). The impact that this risk can have is therefore significant, and underestimated by the participant. The usage of shadow IT should not be tolerated, it should be prohibited. The lack of a legal framework for liabilities may thus not be the only issue, but also the unawareness of the hospital staff of the relation between how they

Table 18: Unique General Information Security risks for each research method, with the number of sources that mentioned it

Systematic literature research	#	**Interviews**	#
Security policies are not explicitly defined	2	Shadow IT	1
Not all security measures are standardized	1	IT department is underfunded and overworked	1
No data transfer policies	1		
Lack of legal framework for liability issues	1		

conduct their business and the laws and regulations.

5.2 Access to Programs and Data

In this category, most technical risks, such as the logging of data, were not mentioned by the participants. A likely reason for this is that the technical of risks are the responsibility of the system and database administrators - as they work on the operating system and database - and none of the interview participants had this role considering the interviews were concentrated on employees who work directly with Epic. Human error, such as leaving a laptop unlocked or leaving a laptop in a public place, was also not mentioned by the participants. That it was not mentioned as a risk is interesting as some of the participants did mention several risks that users pose, such as the use of weak passwords and users having outdated work laptops. However, human errors that participants did focus on were that users may wrongfully have extensive privileges or an incorrect user role.

A shortcoming of the literature is that there was no mention of accounts that are not linked to a staff member, and are used by multiple staff members. Likewise, the only measures specified in literature to prevent unjustified access to a medical record were limited to the logging of whom accessed which medical record. There was no mention of the treatment relationship that has to be established between the healthcare providers (staff members) and the patients, nor the break-the-glass procedure that would be activated if this was not the case. The difficulty of verifying whether a staff member accessed a medical record justifiably is also not discussed in literature. A participant stated that this could not yet be done automatically, and therefore required a lot of time to check. It was also mentioned that even if a treatment relationship is established, accessing a record may still be unjustified, which is another risk that the literature did not mention. Furthermore, although several articles mentioned that staff may not follow security protocols, specific circumstances in which this may happen were not referred to. The participants offered more insight into this, stating circumstances such as a new staff member not yet having access to the system or a staff member lacking the correct access privileges when transferring to another department. Both may result in a staff member using the account of a coworker in order to view the necessary patient information. This risk, however, may be underestimated by participants. If multiple people use an account linked to a single staff member and there is a medical error, it may be impossible to trace who caused (intentionally or not) the error, or the person to whom the account belongs may be incorrectly blamed and face repercussions. The impact of the risk is therefore significant, and more

attention should be paid to preventing this risk. Additionally, participants mentioned the existence of accounts with extensive privileges that were not linked to a single staff member. A possibility not specified by the participants is that these users may not only abuse their privileges by overwriting security protocols and logging into and pretending to be another user, but they may also be able to create an entirely new user and make changes to the system using this new account. It should therefore be questioned why the existence of such shared accounts is necessary, and why these staff members do not have their own accounts.

Table 19: Unique access to programs and data risks for each research method, with the number of sources that mentioned it.

Systematic literature research	#	**Interviews**	#
Human error	5	Accounts that are not linked to a staff member	1
No or incorrect logging of whom accessed data, including data not being electronically signed and no verification who has accessed what data	5		
System has no privilege, user and role management	2		
Unencrypted laptops			

5.3 Continuity

None of the risks in this category which were found in the interviews were unique, meaning all of them had been found in literature . Six risks found in the literature research, however, were not mentioned by the participants. Of these, insufficient training of staff was mentioned by five different scientific articles. A reason this may not have been mentioned by the participants is that many do not directly interact with the users of the system, and therefore would not be involved with any staff training. Despite this, it is still interesting that the literature research found significantly more continuity risks than what the participants mentioned in the interviews, namely 18 risks found in literature and three in the interviews (see Table 17). A reason may be that the description of the risks in literature was more specific than the description the participants gave. For example, multiple participants mentioned the availability of the system and its data as a risk, whereas literature has specified this more towards risks such as: a hardware failure, data not being properly stored and maintained and data being incomplete. This may, at least partially, explain the difference in the number of risks found in literature compared to the interviews.

However, the interviews did offer some unique examples of when a system is not available. Firstly, they mentioned that the Electronic Health Record system is dependent on other software to supply it with data, and if this software has a bug it may cause an error in the Electronic Health Records system. In other words, Epic has a chain dependency on other software that may hinder the availability of Epic. It is worrisome that this was not mentioned in literature, as it can become a significant risk for an Electronic Health Records system. Secondly, the fact that upgrading the system takes the system offline, and thus makes it unavailable, was not mentioned as a risk in literature. Nonetheless, there

were some oversights in the interviews as well. For example, although making back-ups was mentioned as a risk prevention measure, the testing of back-ups was not mentioned. This is important as a backup may not work, because it is either corrupt or contaminated by malware, and should be tested in a sandbox environment. It is also concerning that a participant stated that they do not have a full backup of the Epic, especially as there is no paper trail. This means that if the system does go offline not all the data can be recovered, which is a threat to the continuity of the hospital.

Table 20: Unique continuity risks for each research method, with the number of sources that mentioned it.

Systematic literature research	#	**Interviews**	#
Insufficient training of staff	5		
Application is not maintained	1		
Data is not properly stored and preserved	1		
Decreasing integrity	1		
Human error or failure	1		
Resistance of healthcare providers to technical changes	1		

5.4 Change Management

This category has the most overlap of risks out of all the categories, with only two unique risks total. The first, found in literature, is the risk of a constrained competitive advantage. In the Netherlands there are two major providers of Electronic Health Records for hospitals: Chipsoft (with their system called HiX) and Epic. Epic is the second-largest Electronic Health Records system provider and Hix is the largest provider, being used by 70% of the Dutch hospitals that have an Electronic Health Records system (van Eekeren et al., 2021). Due to the limited choice that hospitals have they may not feel that they have a competitive disadvantage. Participant 2 even stated that they find Epic a good supplier that provides good customer service. Moreover, the competing software - HiX - has usability problems, and there are allegations that the provider Chipsoft exploits their customers (van Kuijk, 2022; Koomen, 2022). For these reasons it is also likely that none of the participants mentioned dependency on their supplier (Epic) as a risk. The second unique risk is that upgrades from Epic may cause a crash, which was not mentioned in literature. This is interesting as literature does state that suppliers often do not support older versions of their software, forcing the customer to upgrade in order to keep receiving support.

When analyzing the interviews, the risk of not having an overview of the full system had as only solution to adapt the change management process. The risk is created as several tools are used to track system modifications, making it hard to create an overview of all the modifications of the system. To create an overview, the hospital should enforce a single tool to track modifications. Another solution to this risk can be that Epic creates a feature with which all the changes can be made. Nonetheless, it is important that the modifications are tracked in a more structural and consistent way to ensure that the system can be understood in the future.

Although this category has the most overlap of risks, the cases in which risks can manifest that were gained during the interviews were not mentioned in literature. For example that a change can have an unexpected impact due to the impact being misjudged or not sufficiently tested. Further, the customizability of Epic was mentioned as a cause that hospitals do not have a full overview of their system. These cases offer more insight into how risks can manifest and thus how they can be prevented.

Table 21: Unique change management risks for each research method, with the number of sources that mentioned it.

Systematic literature research	#	**Interviews**	#
Constrained competitive advantage	3	Upgrades from Epic that may cause a crash	1

5.5 Cyber Security

From the risks found about cyber security it is notable that data encryption was not mentioned by any of the participants either as a risk or as a prevention measure, even though two literature sources did mention it. Two other risks that were not mentioned - that the hospital is unable to recover from a security compromise and that there are no procedures to identify system weaknesses - were also not mentioned. However, participants did state that they had a recovery plan and prevention measures in place to identify system weaknesses. Due to this, it is likely that they did not mention these as risks. The final unique risk of the literature research is the risk of data scavenging, which is when a hacker obtains sensitive information by looking at data residue. A possible explanation that this was not mentioned by the participants can be that, in order to gain access to data residue, a hacker would have to gain access to the system - a risk which was mentioned by multiple participants. Interestingly, one of the participants stated that the patient portal was a risk regarding a hacker gaining access. This way to gain access was not mentioned in literature, as literature only focuses on the Electronic Health Records system itself and not the different components. It is therefore an important addition to literature as it becomes more common for hospitals to have a patient portal. Furthermore, an unique risk not specified in literature is that of saving patient information outside of the Electronic Health Records system, even though this could severely compromise the confidentiality and privacy of the patient. Literature also did not focus on any particular cyber-attack, whereas participants specifically mentioned malware and ransomware as risks to Epic.

Taking a closer look at the interviews, it's important to know that the existence of a backup does not prevent nor solve the threat of a malware attack making the systems' data unavailable. A participant mentioned back-ups as a prevention measure for cyber-attacks. However, malware is usually already on a network for a while before it activates. Therefore, there is a high probability the malware would also be on the backup. Hospitals should therefore take this into account when establishing a cyber-security recovery plan. Next to that, participant 3 made a notable comment about cyber security, namely:

"It will cause another risk if it (the attack) compromises the integrity of the system. Then you get risks on things like the patient data. But well, that won't happen anytime soon. I'm saying that, but of course it's always possible."

With this comment they imply that they do not expect a successful cyber-security attack to take place in the near future. However, the Dutch data protection authority ("Autoriteit Persoonsgegevens") reported in 2022 that the health and well-being sector has the highest amount of cyber-attacks, namely 23% of all reported attacks. They also stated that the Netherlands has the relatively highest number of data leaks (compared to the number of citizens), and stresses the importance of cyber security (Autoriteit Persoonsgegevens, 2022). It could therefore be concluded that even IT staff does not have a realistic view of the cyber security risks.

Table 22: Unique cyber security risks for each research method, with the number of sources that mentioned it.

Systematic literature research	#	**Interviews**	#
Data is not encrypted	2	Patient information is saved outside of Epic	1
Hospital is unable to recover from security compromise	1	Security of the patient portal	1
No procedures to identify system weaknesses	1		
Transparent physical security measures	1		
Data scavenging	1		

5.6 Supplier Management

This category has the highest amount of unique risks, 12 from the literature research and 3 from the interviews. The unique risks that were mentioned the most, namely a competitive disadvantage compared to newer technologies, is likely not named because there are only two major EHR system providers in the Netherlands, as described in the previous subsection about the change management risks (section 5.4). The dependence on Epic for maintenance was also not mentioned by participants, with Participant 3 even stating that they were happy with the support that Epic provided. Similarly, the risks relating to the hospital running an older version of Epic are not relevant, as Epic forces its customers to upgrade to the new versions they release. About the third unique literature research risk, namely the safety implications of an upgrade, a participant explained that they extensively test any upgrade from Epic in a test environment. This offers them more insight into any implications, not just the safety implications, that the upgrade has and to modify the system and/or upgrade to work properly with the hospital's Epic version. As for the unique risks that were found in the interviews, it is interesting that the literature did not mention the risk of the supplier and customer being stationed in a different country, and therefore having to adhere to different laws and regulations. This would be a valuable addition to literature, especially as a participant stated that their hospital did have to check if every update complied with the Dutch (and European) regulations.

Table 23: Unique supplier management risks for each research method, with the number of sources that mentioned it.

Systematic literature research	#	**Interviews**	#
Competitive disadvantage compared to new(er) technologies	3	Different laws and regulations in the United States and the Netherlands	2
Dependence on provider for maintenance	2	Third party management	1
Safety implications of the software and/or its updates are not clear	2		
Access to data is slow	1		
Records are not instantly updated	1		
Third parties using data in a way it was not intended	1		
Maintenance and support only if frequent updates are done	1		
No support for older version	1		
Increased volume and complexity with each update	1		
Asynchronous updates	1		
Poor custom code	1		
Patient data is not distinguishable from other data	1		

5.7 General differences

When comparing all the risks found in literature to all the risks found during the interviews, the literature overall focuses more on the risks on paper (i.e. policies) and the participants focused more on how IT is executed in practice. For example, two of the general information security risks specified in literature concern the policies regarding security whereas the participant focused on more practical risks such as how you should handle shadow IT. A shortcoming of only focusing on policies is that literature also does not specify risks further than a general description, such as the risk of hardware failure, whereas during the interviews specific cases were described on how a risk could manifest. It was also noted that, when naming examples of risk manifestations, scientific articles referred to news articles. The examples they named are therefore often more extreme cases, as small cases - such as a file accidentally being uploaded to the wrong medical record - are not reported in the news. Literature may thus provide an unrealistic view of the reality and of the risk, as they only present the worst-case scenarios and in this fail to describe less impact full, but more often occurring, examples of when a risk can manifest. Moreover, the literature rarely specified prevention measures and focuses solely on naming the risks. During the interviews it was inquired which measures were taken to prevent the risk or minimize its impact, resulting in a more detailed overview of each risk. However, literature did specify more technical risks. This is likely because these risks did not align with the job responsibilities of the participants, and therefore they did not name that as risks. This means that, nonetheless, literature offered a larger variety of risks than the interviews. Thus overall, the interviews provided a more detailed insight into the risks, describing when it can manifest and how hospitals are trying to prevent

and minimize them, whereas literature offered a larger range of risks and covered technical aspects which the participants did not specify.

Chapter 6

Conclusion

In this chapter, the discussion and limitations will be discussed, as well as the findings of the research. The implications of this research will also be mentioned, and suggestions for future research will be given.

6.1 Discussion and Limitations

This section discusses the results as well as the limitations of this research, starting with the scope. The scope of this research was limited to the usage of the Epic system in hospitals in the Netherlands, wherefore it may not be representative of the general risks of hospital EHR systems and Epic around the world. One aspect that may result in different risks, is the size of Dutch hospitals. In the United States there are hospitals that have a significantly higher bed count than those in the Netherlands, which may result in different risks (as they have more staff as well as a more elaborate system) and a more profound risk impact. For comparison, the hospital with the highest bed count in the Netherlands - Erasmus MC - has 1350 beds (Inter-Change, 2021), whereas the highest bed count in the United States is 2247 beds (in the AdventHealth Orlando hospital) (Definitive Healthcare, 2023). It is likely that, among other things, the difference in hospital size between Dutch and American hospitals results in the hospitals having - and possibly prioritizing - different risks.

Another point of discussion is that only the risks of the Epic system were studied. Another EHR system can have different risks, as was highlighted in section 5.4. The system HiX, a competitor of Epic, was shortly mentioned here. One of the differences that was discussed was vendor dependency. Whereas during the interviews one of the participants praised Epic as a vendor, the vendor of Hix is accused of exploiting hospitals (van Kuijk, 2022; Koomen, 2022).

The participants are the final discussion point and limitation of this research. The participants can be split into three different aspects: 1) the number of participants, 2) the distribution of the participants over the hospitals, and 3) the job roles of the participants. The first limitation is the number of participants. The sample size in qualitative research should aim to achieve saturation, which is when no new information is discovered with another sample (in this case, another interview) (Mason et al., 2010). This research did not achieve saturation, as unique risks were mentioned by all the participants. However,

the goal of this research was to identify the differences between literature and practice. Despite saturation not being achieved, differences were still found between the risks specified by literature and those specified by participants. It can therefore be concluded that the results of the research are valid.

The second participant discussion point is the distribution of the participants over the hospitals. Participants working at three different hospitals were interviewed, but 3 of the participants worked at the same hospital. It could therefore be possible that the risks exceedingly represent the circumstances of that specific hospital. However, there was an overlap of the risks that were specified by these participants and those mentioned by the other two, meaning that the risks of Epic are partially similar across different hospitals. That the risks did not have a complete overlap is related to the third discussion point regarding the participants, namely their job roles. Due to the participants having different roles and responsibilities, they are concerned with different risks and therefore are unlikely to have a full overlap in the risks that they mention. Another limitation relating the their job roles is that literature provided more technical risks than the participants. If a participant in a more technical role - such as system administrator - had been interviewed, these risks would likely also be mentioned by during the interviews. It is therefore a limitation of the research that no participant in this role was interviewed.

Despite the limitations and discussion points regarding the participants, there are several factors that indicate that the results of this research are reproducible with more participants. First of all, if a participant stated that a risk had a high priority, it was mentioned by at least one other participant. This shows that, despite the different roles of the participants, they agree on which risks are a threat to Epic. Secondly, there was also an overlap in the risks mentioned outside of the highest priority risks, further showing that the participants agreed on the risks of Epic. It is therefore likely that, if this research is reproduced with more participants, it will have similar results.

6.2 Conclusion

The main research question of this research is:

What are the differences between literature and the users' perception about the perceived information technology and security risks of Epic in hospitals in the Netherlands?

In this research, the differences were found to be:

- Literature focuses more on the risks on paper, whereas interview participants focus on the risks that occur when IT is done in practice. This indicates that there is a disconnect between the risks that are identified by researchers and those identified in practice.
- Literature does not specify risks beyond a general description, with little details of how a risk can manifest.
- When literature does give examples of risk manifestations, they are of cases that made the news (as they reference news articles). This does not give a full nor

accurate overview of the risk, as it only describes the most serious cases but not the smaller - and possibly more often occurring - cases in which a risk manifests.

- Literature often does not specify prevention measures for risks.
- Literature mentioned more technical risks than the participants, which is due to the roles of the participants, as will be discussed in the next section (section 6.1).

It can be concluded that the literature offered a larger variety of risks, whereas the interviews resulted in a deeper understanding and more detailed description of the risks. In literature, risks are mentioned with a short description and one or two news articles to illustrate how the risk may manifest. The interviews provided different examples of how a risk could manifest with specific cases that had happened or were likely to happen, and prevention measures that the hospitals have implemented to prevent the risks. To demonstrate the importance of having a comprehensive risk description, the risks of 'not clearly defining security policies' and 'staff not following security policies' - which are specified in literature - and the risk of shadow IT - described by a participant - can be used. The risk of shadow IT, and the usage of shadow IT, exists despite the hospitals having protocols for requesting new functionalities for Epic and policies that prohibit the use of shadow IT. Although literature specified 'staff not following security policies' as a risk, this risk description is too general for any hospital to act upon (for example, make prevention measures). The description fails to mention how this may happen, what the impact may be, and how to prevent it. The more detailed risk descriptions provided by the participants do present this information and therefore give the information that is needed to more accurately assess a risk. This example also shows that literature is more focused on the risks on paper, whereas participants are more focused on the risks in practice. Literature tries to prevent the risk of shadow IT by having clearly defined policies, which in this case is not effective, and when that does not work it only specifies as another risk that staff may not adhere to the policies. However, it fails to mention how and why any of these risks may manifest. The risk descriptions that were gained during the interviews, on the other hand, largely focused on these factors.

6.3 Implications

The results of this research imply that there is a gap between literature and practice regarding the risks of Epic, and possibly other Electronic Health Record systems. Although most of the risks mentioned by the participants were also specified in the literature, some important risks - such as the risk of different laws and regulations if the customer and supplier are in a different country - are missing from the literature. Moreover, this research presents more insights into the context of the risks by providing more cases in which risks can manifest and how to prevent them. Especially the case examples that have not been reported on by news agencies are valuable, as they were not found in the scientific articles. This research also provides insight into the priority ranking of the risks, as the participants were asked which risks form the highest threat(s) to hospitals. Thus, this research emphasizes the importance of interviews in order to gain insight into how risks are perceived in practice.

6.4 Future work

As stated in the limitations above, this research focused on the Epic system in Dutch hospitals. In future research it would be valuable to also conduct interviews in hospitals that use other EHR systems in order to get a better overview of the EHR risks in the Netherlands. It would also be valuable to not only focus on the EHR systems in hospitals, but on the ones in other healthcare organizations as well. Moreover, future research could focus on EHR systems in different countries, in order to gain a more thorough depiction of the risks of EHR systems. However, when doing this it is important to take into account that the manner in which health care is conducted as well as the laws and regulations differentiate per country.

Another factor for future research could focus on is to have a larger sample size. As stated in the limitations section, saturation was not achieved in this research. It would be valuable for another research to achieve this. Furthermore, the interview strategy could be changed. In this research, the risks found in the literature were not mentioned to the participants in order to prevent bias. Future research could name the risks that were found and possibly discuss these with the participants.

Despite the points made above, this study shows that there is a gap between the risks as perceived in literature and those in real life. The literature lacks detailed overviews of risks and does not describe the situations in which risks can manifest. It also often fails to describe how a risk should be prevented. This study thus showed where literature can make improvements, and how the risks of the Electronic Health Records system Epic are perceived in practice.

Chapter 7

Bibliography

Adolph, W. S. (1996). Cash cow in the tar pit: Reengineering a legacy system. *IEEE Software*, 13:41–47.

Aleksandrova, S. V., Aleksandrov, M. N., and Vasiliev, V. A. (2018). Business continuity management system. In *2018 IEEE International Conference" Quality Management, Transport and Information Security, Information Technologies"(IT&QM&IS)*, pages 14–17. IEEE.

Amsterdam UMC (n.d.). Fusie. *amsterdamumc.org*. `https://www.amsterdamumc.org/nl/organisatie/fusie.htm`.

Anad, A. and Chin, F. (2022). Code grey: Inside a 'catastrophic' it failure at the queensway carleton hospital. *CBC*. `https://www.cbc.ca/news/canada/ottawa/queensway-carleton-hospital-doctors-network-outage-1.6656370`.

Anoshiravani, A., Gaskin, G. L., Groshek, M. R., Kuelbs, C., and Longhurst, C. A. (2012). Special requirements for electronic medical records in adolescent medicine. *Journal of Adolescent Health*, 51:409–414.

Anthony, B., Pa, N. C., Nor, R. N. H., and Josoh, Y. Y. (2016). A risk assessment model for collaborative support in software management. *2015 9th Malaysian Software Engineering Conference, MySEC 2015*, pages 217–223.

Ash, J. S., Berg, M., and Coiera, E. (2004). Some unintended consequences of information technology in health care: The nature of patient care information system-related errors. *Journal of the American Medical Informatics Association*, 11:104–112.

Ashenden, D. (2008). Information security management: A human challenge? *Information security technical report*, 13(4):195–201.

Autoriteit Persoonsgegevens (2020). Jaarrapportage meldplicht datalekken 2019. `https://autoriteitpersoonsgegevens.nl/uploads/imported/jaarcijfers_meldplicht_datalekken_2019.pdf`.

Autoriteit Persoonsgegevens (2022). Jaarrapportage meldplicht datalekken 2021. `https://autoriteitpersoonsgegevens.nl/uploads/imported/datalekkenrapportage_ap_2021.pdf`.

Autoriteit Persoonsgegevens (n.d.). About the dutch dpa. https://autoriteitpersoonsgegevens.nl/en/about-the-dutch-dpa.

Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*, 253:1–13.

Azman, T. I., Pa, N. C., Nor, R. N. H., and Jusoh, Y. Y. (2019). Assessing the instrument reliability and validity of risk mitigation for anti software ageing model during software maintenance. *International Conference on Research and Innovation in Information Systems, ICRIIS*, December-2019.

Bakar, H. K. A. and Razali, R. (2013). A preliminary review of legacy information systems evaluation models. *International Conference on Research and Innovation in Information Systems, ICRIIS*, pages 314–318.

Bannerman, P. L. (2008). Risk and risk management in software projects: A reassessment. *Journal of Systems and Software*, 81:2118–2133.

Benhamou, P. Y. (2011). Improving diabetes management with electronic health records and patients' health records. *Diabetes and Metabolism*, 37.

Bennett, K. (1995). Legacy systems: Coping with success. *IEEE Software*, 12:19–23.

Bisbal, J., Lawless, D., Wu, B., and Grimson, J. (1999). Legacy information systems: issues and directions. *IEEE Software*, 16:103–111.

Bisbal, J., Lawless, D., Wu, B., Grimson, J., Wade, V., Richardson, R., and O'Sullivan, D. (1997). Overview of legacy information system migration. *Proceedings of the Asia-Pacific Software Engineering Conference and International Computer Science Conference, APSEC and ICSC*, pages 529–530.

Blakley, B., Mcdermott, E., Morganchase, J. P., and Geer, D. (2002). Information security is information risk management. *Proceedings of the 2001 workshop on New security paradigms - NSPW '01*.

Boehm, B. W. (1989). Software risk management. In *European Software Engineering Conference*, pages 1–19. Springer.

Boehm, B. W. (1991). Software risk management: Principles and practices. *IEEE Software*, 8:32–41.

Borzekowski, R. (2009). Measuring the cost impact of hospital information systems: 1987–1994. *Journal of Health Economics*, 28:938–949.

Brodie, M. L. and Stonebraker, M. (1995). *Migrating legacy systems: gateways, interfaces the incremental approach*. Morgan Kaufmann Pub.

Brooke, C. and Ramage, M. (2001). Organisational scenarios and legacy systems. *International Journal of Information Management*, 21:365–384.

Bryman, A. and Bell, E. (2015). *Business research methods (Fourth)*. Oxford University Press.

Buchanan, R. L. and Whiting, R. C. (1998). Risk assessment: A means for linking haccp plans and public health. *Journal of Food Protection*, 61:1531–1534.

Carney, D. J., Morris, E. J., and Place, P. R. (2003). Identifying commercial off-the-shelf (cots) product risks: the cots usage risk evaluation.

Chen, G., Wang, K., Tan, J., and Li, X. (2019). A risk assessment method based on software behavior. *2019 IEEE International Conference on Intelligence and Security Informatics, ISI 2019*, pages 47–52.

Chipsfot (n.d.). About chipsoft. *chipsoft.com*. `https://www.chipsoft.com/about-us`.

Chowdhury, A. A. M. and Arefeen, S. (2011). Software risk management: importance and practices. *IJCIT, ISSN*, pages 2078–5828.

Comella-Dorda, S., Wallnau, K., Seacord, R. C., and Robert, J. (2000). A survey of legacy system modernization approaches.

Costagliola, G., Francese, R., and Scanniello, G. (2003). A visual system supporting software reuse in the banking legacy system context. *International Journal of Software Engineering and Knowledge Engineering*, 13:83–101.

Definitive Healthcare (2023). What are the largest U.S. hospitals by bed count? `https://www.definitivehc.com/resources/healthcare-insights/us-hospitals-most-beds#:~:text=AdventHealth%20Orlando%20is%20the%20largest,discharges%20and%20net%20patient%20revenue`.

DigiD (n.d.). What is digid? *DigiD*. `https://www.digid.nl/en/what-is-digid/`.

Donner, R. S. and Bickley, H. (1993). Problem-based learning in american medical education: an overview. *Bulletin of the Medical Library Association*, 81:294.

Els, F. and Cilliers, L. (2017). Improving the information security of personal electronic health records to protect a patient's health information. *2017 Conference on Information Communication Technology and Society, ICTAS 2017 - Proceedings*.

Epic (n.d.). About — epic. *epic.com*. `https://www.epic.com/about/`.

European Parliament and Council of the European Union (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council. of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Retrieved March 20, 2023, from `https://data.europa.eu/eli/reg/2016/679/oj`.

Fairley, R. (1994). Risk management for software projects. *IEEE Software*, 11:57–67.

Foo, S. W. and Muruganantham, A. (2000). Software risk assessment model. *Proceedings of the 2000 IEEE International Conference on Management of Innovation and Technology:*, 2:536–544.

Fürnweger, A., Auer, M., and Biffl, S. (2016). Software evolution of legacy systems: A case study of soft-migration. *ICEIS 2016 - Proceedings of the 18th International Conference on Enterprise Information Systems*, 1:413–424.

Gao, J., Bai, X., Tsai, W. T., and Uehara, T. (2013). Saas testing on clouds - issues, challenges, and needs. *Proceedings - 2013 IEEE 7th International Symposium on Service-Oriented System Engineering, SOSE 2013*, pages 409–415.

Goseva-Popstojanova, K., Hassan, A., Guedem, A., Abdelmoez, W., Nassar, D. E. M., Ammar, H., and Mili, A. (2003). Architectural-level risk analysis using uml. *IEEE Transactions on Software Engineering*, 29:946–959.

Gude, W. and van Luxemburg, A. (2020). Coronacrisis: de effecten op digitalisering in de zorg.

Harman, L. B., Flite, C. A., and Bond, K. (2012). Electronic health records: privacy, confidentiality, and security. *AMA journal of ethics*, 14(9):712–719.

Heart, T. (2010). Who is out there? exploring the effects of trust and perceived risk on saas adoption intentions. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, 41:49–68.

Heemstra, F. J. and Kusters, R. J. (1996). Dealing with risk: A practical approach. *Journal of Information Technology*, 11:333–346.

Hewett, R. (2005). Information-based risk assessment software architecture. *IEEE International Engineering Management Conference*, II:574–578.

Hoerbst, A. and Ammenwerth, E. (2010). Electronic health records: A systematic review on quality requirements. *Methods of Information in Medicine*, 49:320–336.

Hussain, S. M., Bhatti, S. N., and Rasool, M. F. U. (2017). Legacy system and ways of its evolution. *International Conference on Communication Technologies, ComTech 2017*, pages 56–59.

Iakovidis, I. (1998). Towards personal health record: current situation, obstacles and trends in implementation of electronic healthcare record in europe. *International Journal of Medical Informatics*, 52:105–115.

ICT&health (2022). Datalek asz: half miljoen medische bestanden overschreven. *ICT&health*. `https://icthealth.nl/nieuws/datalek-asz-half-miljoen-medische-bestanden-overschreven/`.

Inter-Change (2021). Top 10 grootste ziekenhuizen van Nederland. `https://www.inter-change.nl/nieuws/ziekenhuizen/top-10-grootste-ziekenhuizen-van-nederland/`.

Ismail, A., Jamil, A. T., Rahman, A. F. A., Bakar, J. M. A., Saad, N. M., and Saadi, H. (2010). The implementation of hospital information system (his) in tertiary hospitals in malaysia: a qualitative study. *Malaysian Journal of Public Health Medicine*, 10:16–24.

Kenton, W. (2022). What are the big 4 accounting firms? Definition and critique. *Investopedia*. `https://www.investopedia.com/terms/b/bigfour.asp#citation-5`.

Khan, M., Ali, I., Mehmood, W., Nisar, W., Aslam, W., Shafiq, M., and Choi, J. G. (2021). Cmmi compliant modernization framework to transform legacy systems. *Intelligent Automation and Soft Computing*, 27:311–331.

Khatri, N. and Gupta, V. (2016). Effective implementation of health information technologies in u.s. hospitals. *Health Care Management Review*, 41:11–21.

Kierkegaard, P. (2011). Electronic health record: Wiring europe's healthcare. *Computer Law Security Review*, 27:503–515.

Koomen, W. (2022). Dodelijke zorg [film]. *Talent United Film & TV, KRO-NCRV*. https://www.npostart.nl/2doc/15-09-2022/KN_1727593.

KPMG (n.d.a). KPMG — LinkedIn. https://www.linkedin.com/company/kpmg/?trk=public_profile_experience-item_profile-section-card_subtitle-click&originalSubdomain=lk.

KPMG (n.d.b). KPMG toonaangevend in audit, assurance, digitalisering en tax. https://kpmg.com/nl/nl/home.html.

Kuckartz, U. (2019). Qualitative text analysis: A systematic approach. *Compendium for early career researchers in mathematics education*, pages 181–197.

Lluch, M. (2011). Healthcare professionals' organisational barriers to health information technologies—a literature review. *International Journal of Medical Informatics*, 80:849–862.

Lucia, A. D., Fasolino, A. R., and Pompella, E. (2001). A decisional framework for legacy system management. *IEEE International Conference on Software Maintenance, ICSM*, pages 642–653.

Lyytinen, K., Mathiassen, L., and Ropponen, J. (1998). Attention shaping and software risk—a categorical analysis of four classical risk management approaches. *Information Systems Research*, 9:233–255.

Maastricht UMC (2023). Maastricht umc+ kiest voor het elektronisch patiëntendossier van epic. *mumc.nl*. https://www.mumc.nl/actueel/nieuws/maastricht-umc-kiest-voor-het-elektronisch-patientendossier-van-epic.

Mason, M. et al. (2010). Sample size and saturation in phd studies using qualitative interviews. In *Forum qualitative Sozialforschung/Forum: qualitative social research*, volume 11.

Matthiesen, S. and Bjørn, P. (2015). Why replacing legacy systems is so hard in global software development: An information infrastructure perspective. *CSCW 2015 - Proceedings of the 2015 ACM International Conference on Computer-Supported Cooperative Work and Social Computing*, pages 876–890.

McLean, E., Cogswell, M., Egli, I., Wojdyla, D., and Benoist, B. D. (2009). Worldwide prevalence of anaemia, who vitamin and mineral nutrition information system, 1993–2005. *Public Health Nutrition*, 12:444–454.

McMullen, P. C., Howie, W. O., Philipsen, N., Bryant, V. C., Setlow, P. D., Calhoun, M., and Green, Z. D. (2014). Electronic medical records and electronic health records: Overview for nurse practitioners. *The Journal for Nurse Practitioners*, 10:660–665.

Medius.nl (n.d.). What is supplier management? *Medius*. https://www.medius.com/glossary/what-is-supplier-management/.

Meho, L. I. and Yang, K. (2007). Impact of data sources on citation counts and rankings of lis faculty: Web of science versus scopus and google scholar. *Journal of the american society for information science and technology*, 58(13):2105–2125.

Mehta, A. and Heineman, G. T. (2002). Evolving legacy system features into fine-grained components. *Proceedings of the 24th international conference on Software engineering - ICSE '02*.

Merola, L. (2006). The cots software obsolescence threat. *Proceedings - Fifth International Conference on Commercial-off-the-Shelf (COTS)-Based Software Systems*, 2006:127–133.

Metzger, J. N., Fjeld, R. A., Hammonds, J. S., and Hoffman, F. O. (1998). Evaluation of software for propagating uncertainty through risk assessment models. *Human and Ecological Risk Assessment: An International Journal*, 4:263–290.

Morisio, M. and Torchiano, M. (2002). Definition and classification of cots: A proposal. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2255:165–175.

Mount, C. D., Kelman, C. W., Smith, L. R., and Douglas, R. M. (2000). An integrated electronic health record and information system for australia? *Medical Journal of Australia*, 172:25–27.

Narayana Samy, G., Ahmad, R., and Ismail, Z. (2010). Security threats categories in healthcare information systems. *Health informatics journal*, 16(3):201–209.

Nguyen, L., Bellucci, E., and Nguyen, L. T. (2014). Electronic health records implementation: An evaluation of information system impact and contingency factors. *International Journal of Medical Informatics*, 83:779–796.

NOS Nieuws (2018). Tientallen onbevoegden bekeken medisch dossier barbie. *NOS*. `https://nos.nl/artikel/2225867-tientallen-onbevoegden-bekeken-medisch-dossier-barbie`.

NOS Nieuws (2019). Hoge boete voor haga-ziekenhuis na rel rond dossier barbie. *NOS*. `https://nos.nl/artikel/2293700-hoge-boete-voor-haga-ziekenhuis-na-rel-rond-dossier-barbie`.

Paakkari, L. and Okan, O. (2020). Covid-19: health literacy is an underestimated problem. *The Lancet Public Health*, 5:e249–e250.

Parnas, D. L. (1994). Software aging. *Proceedings - International Conference on Software Engineering*, pages 279–287.

Port, D. and Chen, S. (2004). Assessing cots assessment: how much is enough? *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2959:183–198.

Rahman, M. and Kreider, C. (2012). Information security principles for electronic medical record (emr) systems.

Raposo, V. L. (2015). Electronic health records: Is it a risk worth taking in healthcare delivery? *GMS health technology assessment*, 11.

Redmill, F. (2004). Analysis of the cots debate. *Safety Science*, 42:355–367.

RIVM (2022). Ziekenhuiszorg — aanbod — instellingen. *Vzinfo.nl*. `https://www.vzinfo.nl/ziekenhuiszorg/aanbod/instellingen`.

Roehrs, A., Costa, C. A. D., Righi, R. D. R., and Oliveira, K. S. F. D. (2017). Personal health records: A systematic literature review. *Journal of Medical Internet Research*, 19.

RTL Nieuws (2018). Ziekenhuis schrikt van inbreuk op dossier barbie: mogelijk ontslag medewerkers. *RTLnieuws.nl*. `https://www.rtlnieuws.nl/nieuws/nederland/artikel/4139781/ziekenhuis-schrikt-van-inbreuk-op-dossier-barbie-mogelijk-ontslag`.

Samy, G. N., Ahmad, R., and Ismail, Z. (2009). Threats to health information security. *5th International Conference on Information Assurance and Security, IAS 2009*, 2:540–543.

Samy, G. N., Ahmad, R., and Ismail, Z. (2010). Security threats categories in healthcare information systems. *Health Informatics Journal*, 16:201–209.

Schatz, D., Bashroush, R., and Wall, J. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law*, 12(2):8.

Schiza, E. C., Fakas, G. J., Pattichis, C. S., Petkov, N., and Schizas, C. N. (2016). Data protection issues of integrated electronic health records (ehr). In *XIV Mediterranean Conference on Medical and Biological Engineering and Computing 2016: MEDICON 2016, March 31st-April 2nd 2016, Paphos, Cyprus*, pages 787–790. Springer.

Shirabad, J. S., Lethbridge, T. C., and Matwin, S. (2003). Mining the maintenance history of a legacy software system. *IEEE International Conference on Software Maintenance, ICSM*, pages 95–104.

Shyur, H. J. (2006). Cots evaluation using modified topsis and anp. *Applied Mathematics and Computation*, 177:251–259.

Smithson, S. and Hirschheim, R. (2017). Analysing information systems evaluation: another look at an old problem. *https://doi.org/10.1057/palgrave.ejis.3000304*, 7:158–174.

Stoneburner, G., Goguen, A., and Feringa, A. (2002). Risk management guide for information technology systems.

Tanwar, S., Parekh, K., and Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and Applications*, 50:102407.

Taylor, H., Artman, E., and Woelfer, J. P. (2012). Information technology project risk management: Bridging the gap between research and practice. *Journal of Information Technology*, 27:17–34.

Tesch, D., Kloppenborg, T. J., and Frolick, M. N. (2007). It project risk factors: the project management professionals perspective. *Journal of computer information systems*, 47:61–69.

Tohidi, H. (2011). The role of risk management in it systems of organizations. *Procedia Computer Science*, 3:881–887.

Turan, A. H. and Palvia, P. C. (2014). Critical information technology issues in turkish healthcare. *Information and Management*, 51:57–68.

Uwizeyemungu, S. and Poba-Nzaou, P. (2017). Health information exchange and related it-security practices in european hospitals. *ICISSP 2017 - Proceedings of the 3rd International Conference on Information Systems Security and Privacy*, 2017-January:538–545.

van Eekeren, P., Meijer, S., and de Bruyn, W. (2021). Epd-marktinventarisatie ziekenhuizen 2021: consolidatie epd-markt zet door. `https://mxi.nl/kennis/541/epd-marktinventarisatie-ziekenhuizen-2021-consolidatie-epd-markt-zet-door`.

van Kuijk, J. (2022). Ongezond: de leverancier van gebruiksonvriendelijke ziekenhuis-ict heeft min of meer een monopolie. *Volkskrant*. `https://www.volkskrant.nl/wetenschap/ongezond-de-leverancier-van-gebruiksonvriendelijke-ziekenhuis-ict-heeft-min-of-meer-een-monopolie~b80197ec/`.

van Lonkhuyzen, L. (2022). Ziekenhuizen voelen zich klemgezet door softwarebouwer. *NRC*. `https://www.nrc.nl/nieuws/2022/05/04/ziekenhuizen-voelen-zich-klemgezet-door-softwarebouwer-a4122715?t=1670599056`.

Verkerk, J. (2022). Grote storing bij ziekenhuis maastricht, duizenden behandelingen gaan niet door. *NRC*. `https://www.nrc.nl/nieuws/2022/09/08/grote-storing-bij-ziekenhuis-maastricht-poliklinieken-dicht-a4141162`.

Vidger, M. R. and Dean, J. (1997). An architectural approach to building systems from cots software components. pages 99–131.

Webster, J. and Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS quarterly*, pages xiii–xxiii.

Wester, J. (2022). Ziekenhuis veroordeeld voor falende bescherming medische dossiers. *NRC Handelsblad*. `https://www.nrc.nl/nieuws/2022/09/21/ziekenhuis-veroordeeld-voor-falende-bescherming-medische-dossiers-a4142728?t=1683899586`.

Wolfswinkel, J. F., Furtmueller, E., and Wilderom, C. P. (2013). Using grounded theory as a method for rigorously reviewing literature. *European journal of information systems*, 22:45–55.

Wu, M., Hou, H., Liu, C., and Ying, J. (2006). Cots-based system's obsolescence risk evaluation. *Proceedings - 2006 10th International Conference on Computer Supported Cooperative Work in Design, CSCWD 2006*, pages 240–244.

Xia, L., Yang, J., Wang, H., and Hou, X. (2018). Safety analysis and risk assessment of lpar software system. *Proceedings - 12th International Conference on Reliability, Maintainability, and Safety, ICRMS 2018*, pages 150–154.

Yang, K. and Meho, L. I. (2006). Citation analysis: a comparison of google scholar, scopus, and web of science. *Proceedings of the American Society for information science and technology*, 43(1):1–15.

Yusoh, Z. I. M. and Tang, M. (2010). A penalty-based genetic algorithm for the composite saas placement problem in the cloud. *2010 IEEE World Congress on Computational Intelligence, WCCI 2010 - 2010 IEEE Congress on Evolutionary Computation, CEC 2010*.

Zhao, Y., Xiang, J., Xiong, S., Wu, Y., An, J., Wang, S., and Yu, X. (2016). An experimental study on software aging in android operating system. *Proceedings - 2015 2nd International Symposium on Dependable Computing and Internet of Things, DCIT 2015*, pages 148–150.

Ziekenhuis Amstelland (2022). Ziekenhuis amstelland neemt epic als nieuw elektronisch patiëntendossier (epd) in gebruik. *ziekenhuisamstelland.nl*. `https://ziekenhuisamstelland.nl/nl/nieuws/actueel/ziekenhuis-amstelland-neemt-epic-als-nieuw-elektronisch-patientendossier-epd-in-gebruik/`.

Ángel DÍaz De León Guillén, M., Morales-Rocha, V., and Martínez, L. F. F. (2020). A systematic review of security threats and countermeasures in saas. *Journal of Computer Security*, 28:635–653.

Appendix A

Literature Search

A.1 Keywords and synonyms

Table 24: Keywords and synonyms

Research keyword	**Synonyms**
Legacy	Legacy, old, ageing
Risk	Risk, threat, problem, issue
System	System, Information System (IS), software, Information Technology (IT)
Hospital IS	Hospital Information System (HIS), Health Information Technology (HIT), digital health, healthcare technology management, health informatics, health technology, medical information system
COTS	Commercial-Off-The-Shelf (COTS), third party, Software as a Service (SaaS)
Assessment	Assessment, assess, evaluation, impact, consequences
Electronic Health Record (EHR)	Electronic Medical Record (EMR), Electronic Patient Records (EPR), Summary Health Record (SHR), Personal Health Record (PHR)

A.2 Papers found

The '#' column in the table refers to the query number, which can be found in Table 1 on page 9. Furthermore, the database Web of Science is abbreviated to WoS in the table.

Table 25: Literature Search

#	Date	DB	Results Top 4	Other interesting papers
1	4-okt	WoS	1. Ismail et al. (2010) 2. Turan and Palvia (2014) 3. Samy et al. (2009) 4. Khatri and Gupta (2016)	Uwizeyemungu and Poba-Nzaou (2017); Lluch (2011)
	4-okt	Google Scholar	1. Ash et al. (2004) 2. Paakkari and Okan (2020) 3. Donner and Bickley (1993) 4. McLean et al. (2009)	Blakley et al. (2002)
2	4-okt	WoS	1. Anthony et al. (2016) 2. Hewett (2005) 3. Metzger et al. (1998) 4. Xia et al. (2018)	Aven (2016); Chen et al. (2019); Foo and Muruganantham (2000)
	4-okt	Google Scholar	1. Tohidi (2011) 2. Buchanan and Whiting (1998) 3. Stoneburner et al. (2002) 4. Goseva-Popstojanova et al. (2003)	
3	5-okt	WoS	Top 4 focussed on aspects of risk management not relevant for this research, such as architectural changes to software	
	5-okt	Google Scholar	1. Boehm (1989) 2. Boehm (1991) 3. Bannerman (2008) 4. Lyytinen et al. (1998)	Fairley (1994)
4	7-okt	WoS	1. Fürnweger et al. (2016) 2. Costagliola et al. (2003) 3. Matthiesen and Bjørn (2015) 4. Khan et al. (2021)	
	7-okt	Google Scholar	1. Shirabad et al. (2003) 2. Comella-Dorda et al. (2000) 3. Mehta and Heineman (2002) 4. Smithson and Hirschheim (2017)	Bennett (1995); Bisbal et al. (1999)
4a	25-okt	WoS	1. Fürnweger et al. (2016) 2. Costagliola et al. (2003) 3. Matthiesen and Bjørn (2015) 4. Zhao et al. (2016)	Azman et al. (2019); Bakar and Razali (2013); Brooke and Ramage (2001)

	25-okt	Google Scholar	Top 4 was not relevant as it was focused on the relation between deseases and aging	Parnas (1994)
4b	25-okt	WoS	Top 4 same as for the other queries from 4.	
	25-okt	Google Scholar	1. Shirabad et al. (2003) 2. Lucia et al. (2001) 3. Bisbal et al. (1997) 4. Adolph (1996)	Hussain et al. (2017); Bisbal et al. (1999); Lucia et al. (2001); Adolph (1996)
5	25-okt	WoS	1. Gao et al. (2013) 2. Wu et al. (2006) 3. Port and Chen (2004) 4. Ángel DÍaz De León Guillén et al. (2020)	Merola (2006); Redmill (2004); Wu et al. (2006)
	25-okt	Google Scholar	1. Yusoh and Tang (2010) 2. Carney et al. (2003) 3. Shyur (2006) 4. Heart (2010)	
6	5-apr	WoS	1. Els and Cilliers (2017) 2. Benhamou (2011) 3. Hoerbst and Ammenwerth (2010) 4. Anoshiravani et al. (2012)	McMullen et al. (2014); Kierkegaard (2011); Rahman and Kreider (2012); Schiza et al. (2016); Roehrs et al. (2017)
	5-apr	Google Scholar	1. Iakovidis (1998) 2. Nguyen et al. (2014) 3. Mount et al. (2000) 4. Tanwar et al. (2020)	Harman et al. (2012); Raposo (2015)

Appendix B

Interview Guide

Introductie:

- Naam + master
- Leg uit waar mijn scriptie over gaat en waarom het relevant is
- Vertel dat ik de data ga anonimiseren en vraag om toestemming om op te nemen

Vragen:

1. Persoonlijke ervaring:
   (a) Kan je wat vertellen over de rol die je hebt in het ziekenhuis?
   (b) Hoe lang werk je in deze rol?
   (c) Hoe lang werk je al in het ziekenhuis en wat is je achtergrond?
   (d) Hoe lang heb je al met Epic gewerkt?
2. Ik leg uit wat elke categorie inhoud en geef eventueel 1-2 voorbeelden van risico's. Per risico categorie (2-3 per interview):
   (a) Als je terugdenkt aan het laatste jaar dat je met Epic gewerkt hebt, welke risico's zie je dan binnen deze categorie?
   (b) Per risico:
      i. Zijn er omstandigheden waarin dit risico groter is?
      ii. Wie worden er getroffen door dit risico?
      iii. Wie is er verantwoordelijk voor dit risico?
      iv. In welke mate heeft dit risico plaatsgevonden?
         A. Wat zijn/waren de consequenties van dit risico?
         B. Veroorzaakt dit risico andere risico's?/Heeft dit risico andere risico's veroorzaakt?
         C. Heb je voorbeelden/nog een voorbeeld van hoe dit risico plaats kan vinden?
      v. Zijn er processen en/of procedure om dit risico te voorkomen of te minimaliseren?/Hoe hebben jullie het risico geminimaliseerd?
      vi. Wat hebben jullie nodig om (beter) met deze risico's om te gaan?

(c) Van de risico's die je genoemd hebt, zijn bepaalde risico's belangrijker? [Zo ja, welke en waarom]

3. Zou je nog iets willen toevoegen?

4. Hebben we iets gemist?

Bedankt voor het interview.

Appendix C

Literature Research Risks

General Information security	**Mentioned by**
Security policies are not explicitly defined	Hoerbst and Ammenwerth (2010); Rahman and Kreider (2012)
No data transfer policies	Hoerbst and Ammenwerth (2010)
Not all security measures are standardized	Hoerbst and Ammenwerth (2010)
Lack of legal framework for liability issues	Lluch (2011)
Access to programs and data	
No or inadequate authorization and access control	Hoerbst and Ammenwerth (2010); Rahman and Kreider (2012); Kierkegaard (2011); McMullen et al. (2014); Roehrs et al. (2017); Schiza et al. (2016)
Human error	Harman et al. (2012); Rahman and Kreider (2012); Kierkegaard (2011); McMullen et al. (2014); Raposo (2015)
System has no privilege, user and role management	Harman et al. (2012); Rahman and Kreider (2012); Hoerbst and Ammenwerth (2010)
Security policies are not followed	Kierkegaard (2011); Rahman and Kreider (2012)
Un-encrypted laptops	Kierkegaard (2011)
Abuse of access privileges	Rahman and Kreider (2012)
Accessing and releasing information to outsiders intentionally	Rahman and Kreider (2012)
No/Incorrect logging	Hoerbst and Ammenwerth (2010); Rahman and Kreider (2012); Harman et al. (2012); Schiza et al. (2016)
Continuity	
Finding experts to maintain the system is difficult and expensive	Fürnweger et al. (2016); Comella-Dorda et al. (2000); Adolph (1996)
Insufficient training of staff	McMullen et al. (2014); Raposo (2015)

Power failure/loss	(Samy et al., 2009; Narayana Samy et al., 2010)
Technological obsolescence	(Samy et al., 2009; Narayana Samy et al., 2010)
Hardware failures	(Samy et al., 2009; Narayana Samy et al., 2010)
Software failures	(Samy et al., 2009; Narayana Samy et al., 2010)
Application is not maintained	Hoerbst and Ammenwerth (2010)
Data is not properly stored and preserved	Kierkegaard (2011)
Data is not available	Hoerbst and Ammenwerth (2010)
Deleted data is available in the system	Hoerbst and Ammenwerth (2010)
Data is incomplete	Raposo (2015)
Copy/pasting data which causes a fault in many medical records	Raposo (2015)
Decreasing integrity	Comella-Dorda et al. (2000)
Network infrastructure failures or errors	(Samy et al., 2009)
Human error or failure	Narayana Samy et al. (2010)
Resistance of healthcare providers to technical changes	Lluch (2011)
System increasing in volume the older it gets	Parnas (1994)
Performance degration	Parnas (1994)
Change management	
Hard to change and/or update	Bennett (1995); Fürnweger et al. (2016); Hussain et al. (2017); Bisbal et al. (1997, 1999)
Constrained competitive advantage	Comella-Dorda et al. (2000); Hussain et al. (2017); Bennett (1995)
Maintenance is time-consuming	Bisbal et al. (1997, 1999); Bennett (1995)
Correcting error introduces more errors	Parnas (1994)
Software fosters errors rather than to reduce them	Ash et al. (2004)
Cyber security	
Hackers	McMullen et al. (2014); Harman et al. (2012); Rahman and Kreider (2012); Raposo (2015); Kierkegaard (2011)
Hackers - stealing data	McMullen et al. (2014); Harman et al. (2012); Rahman and Kreider (2012); Raposo (2015); Kierkegaard (2011)
Data is not encrypted	Harman et al. (2012); Rahman and Kreider (2012)
Messages are not encrypted	Hoerbst and Ammenwerth (2010); Kierkegaard (2011)
Disgruntled and disloyal employees	McMullen et al. (2014); Harman et al. (2012)

Hospital is unable to recover from security compromise	Rahman and Kreider (2012)
Loss of data	Kierkegaard (2011)
No procedures to identify system weaknesses	Rahman and Kreider (2012)
Poor password management	McMullen et al. (2014)
Cyber-attacks	(Raposo, 2015)
Transparent physical security measures	McMullen et al. (2014)
Hackers - changing data	(Schiza et al., 2016)
Phishing mails	Kierkegaard (2011)
Accessing and releasing information	Rahman and Kreider (2012)
Hindering accessibility of the system	Rahman and Kreider (2012)
Hindering usability of the system	Rahman and Kreider (2012)
Malicious employees and experts	Ángel DÍaz De León Guillén et al. (2020)
Password stealing	Ángel DÍaz De León Guillén et al. (2020)
Attack from a user, software, or the internet	Ángel DÍaz De León Guillén et al. (2020)
Data scavenging	Ángel DÍaz De León Guillén et al. (2020)
Data loss or leakage	Ángel DÍaz De León Guillén et al. (2020)
Identity theft	Ángel DÍaz De León Guillén et al. (2020)
Supplier management	
Documentation lacking	Bisbal et al. (1999)
Competitive disadvantage compared to new(er) technologies	Comella-Dorda et al. (2000); Hussain et al. (2017)
Black-box	Redmill (2004); Heart (2010)
Maintenance is difficult	Bisbal et al. (1999); Fürnweger et al. (2016)
Dependence on provider for maintenance	Heart (2010); Redmill (2004)
Undesirable/dangerous effects with update	Redmill (2004); Shyur (2006)
Safety implications of the software and/or it's updates are not clear	Redmill (2004); Shyur (2006)
Access to data is slow	Hoerbst and Ammenwerth (2010)
Records are not instantly updated	Hoerbst and Ammenwerth (2010)
Third parties using data in a way it was not intended	Schiza et al. (2016)
No documentation	Redmill (2004); Ángel DÍaz De León Guillén et al. (2020)
Increased financial cost	Redmill (2004)
Maintenance and support only if frequent updates are done	Redmill (2004)
No support for older version	Wu et al. (2006)
No control over composition upgrades	Redmill (2004)
Increased volume and complexity with each update	Redmill (2004)

Asynchronous updates	Redmill (2004)
Poor performance	Shyur (2006)
Poor custom code	Shyur (2006)
Risk of unavailability	Heart (2010)
Patient data is not distinguishable from other data	Hoerbst and Ammenwerth (2010)

Appendix D

Interview Risk Categories

Each interview risk had the subcategories. Some of the risks do no not include all of the subcategories, as it may not have been asked due deviations on the interview guide. The subcategories are:

- When it manifests
- Risk has happened
- Party responsible of the risk
- Example cases
- Consequences of the risk manifesting
- Prevention measures
- Actions taken when the risks manifests
- Circumstances in which the risk is acceptable
- Measures needed in order to reduce to risk
- Other risks that are caused by this risk manifesting

Appendix E

Interview Results

E.1 General Information Security

Data is accurate (integrity)

- When it manifests:
  - Staff members put information of one patient in the medical record of another patient
  - Any information that has to be done manually, outside of the system
- Responsible for integrity of data: the director.
- Examples:
  - Document that has been uploaded has the wrong name (of the patient for example)
  - Notes made about the treatment of the patient are different from the specified treatment
  - Data is most likely put in the wrong medical record with: twins. They have the same birth date, same address, same last name and often their initial(s) are the same as well (e.g. Timmy and Thomas)
  - Faxing information. This is filled in by hand with takes a lot of time and most likely that mistakes are made, for example with the BSN number
- Prevention:
  - Data is passed through many different eyes (the doctor, nurse, receptionist) which mostly catch any mistakes in the medical record. Otherwise it will be caught at the invoice department.
  - All mutations are recorded thorough the day and uploaded in the night
  - It's not possible to fully delete data without admin rights
- Consequence:
  - Need to make a report at the "Autoriteit persoonsgegevens" (the Dutch authority concerned with protecting personal data)

  - Reputation damage
  - Worst case: An operation is done incorrectly based on the medical record. For example the left instead of right knee is operated, or the left instead of right leg is amputated. This is, however, extremely unlikely if someone put information in the wrong medical record, as for this to happen both patients would need to have problems with their knee.

- Acceptable: if it happens once a month for example. Not acceptable: 4 times per day.
- Other risks:
  - Reputation damage

Shadow IT

- Explanation: Programs that have not been approved by the IT department
- How it manifests:
  - IT department is underfunded and overworked
  - Departments can pay for software themselves, which they do without consulting the IT department. Then the IT department is not aware that the software is used
  - Hospital struggles with the identity of staff due to the IT department being overworked
- Prevention:
  - All costs related to IT are assigned to the IT department, through which the IT department will be aware of any programs and services purchased.
  - Raising staff awareness, by making announcement that request them to report shadow IT
  - Controls on (finding) shadow IT
- Consequences:
  - Hospital uses a program (i.e. shadow IT) that did not undergo a data and privacy impact assessment, nor a security assessment. This means that hospital data, possibly confidential data or patient information, is in a program that has not been approved by the IT department and that may not meet the security requirements of the hospital.
  - Patient data in an external system
  - Hospital does not comply with security requirements
  - A former staff member of the hospital still has access to (confidential) data from the hospital. This happens because when a staff member resigns, the team lead has to ensure that the account of said member is revoked/made inaccessible to the staff member as the system is out of the control (or possibly even knowledge) of the IT department.

  - IT department (which is already overworked) has more work as they have to approve the shadow IT
  - The costs of the Shadow IT (for example subscription costs) are subtracted from the department that uses it (instead of the IT department).

- Needed to do better:
  - There will always be shadow IT.

IT department is underfunded and overworked

- How it manifests:
  - High occupancy rate
- Consequence:
  - Little room to no for new projects. The project calendar for the next year is already full before the year starts.
  - Important projects get delayed.
  - People start using shadow IT
  - Shadow IT results in even more work for the IT department
- Other risk that results from this:
  - Shadow IT, as people want a new or additional feature or software, but don't want to wait 1,5 years for it.

E.2 Access to programs and data

Unjustified access to a medical record

- *Number of participants that named the risk: 2*
- **P1:** named this as the highest priority risk
- When it manifests:
  - Very hard to check if access to a medical record by staff was necessary due to how many times patient records are accessed per day (thousands of times). It's impossible to check all of them
  - A staff member accesses a medical record that they are not allowed to access (see example with patients on a department)
  - A staff member accesses a medical record of a patient they do not have a treatment relationship with
  - For IT staff: There are multiple environments that the system uses, user with extensive privileges to multiple of these environments may access them unjustified

- Example:
  - If a patient is hospitalized all staff members in the department they are at are part of their treatment team according to the system, and therefore have access to the patient's medical record (without break-the-glass). However, not all nurses on the department may be actually treating the patient. Nurses are often assigned to beds (for example one to bed 1-4, another to bed 4-8). So nurses have access to medical records of patients they are not treating. Confidentiality can then be broken unnoticed. Becomes more of a risk if the patient and a nurse know each other.
  - Medical staff looks at their own medical record (which is not allowed). Reason for them to do this: in the patient portal not all information is visible (doctors can make certain information not visible to the patient, for example their own notes from an appointment).
    - This is seen as an acceptable risk, also as staff sometimes gets permission from their team leader to view their own records.
  - Medical staff accessing the medical record of a family member or person they know
  - Case about the emergency care secretary that looked into the medical records of the ex of her partner, after which the partner released a book including the ex's medical information.
  - A patient is treated at the emergency care, and therefore does not have a treatment relationship with the staff that helps them
- Prevention:
  - Monitoring accesses *[different ways mentioned of this mentioned by 2 participants]*:
    - Checking who accesses which medical record, although this is hard as there are many accesses per day.
    - Random sample tests for the whole hospital
    - Random sample tests among users with extensive privileges.
  - Look at why staff access a medical record after an invoice has been send to the patient (and therefore the treatment has ended and there is less of a reason for a staff member to access the patients record).
  - Check of last names of patients and medical care to see if medical staff accessed the medical record of a family member. However this is not a solid method as family members can have different last names (for example parents keeping their birth name, and the child having the last name of one of them).
  - Patients can have their record marked as confidential. If this is the case, there will always be a break-the-glass procedure independent of whether or not the staff is part of the treatment team.
  - Spreading awareness (for example the integrity statement)
    - Spreading awareness among staff by explaining what is and is not allowed. *[mentioned by 2 participants]*

    - Spreading awareness that controls are performed on the staffs' activities in the system by regularly asking staff members why they accessed a certain medical record.
    - Staff members have to sign an integrity statement (which states that they will only use the system within the necessity of the job)
  - Checking the rights of admin users.

- Actions taken when it happens:
  - It's hard to determine in hindsight if access was justified
  - Checking if there is a treatment relationship between the staff member and the patient

- Consequences:
  - Staff member that broke the rules has a conversation about it.
  - Patient can make a complaint, in which case the hospital is required to give a detailed (inhoudelijk) reply. The staff member whom the complaint concerns is also required to write down a defense.
  - In the most serious case, the staff member is let go.
  - Hospital is fined
  - Reputation damage

- What is needed to have better prevention:
  - More FTE's that can check if access policies are adhered. Checking if accessing a medical record was justified is difficult and takes time, and it is difficult to set rules as to when it is unjustified. Therefore it is also hard to automate.
  - Hypothesis about (un)justified access, which would make it possible to automate (part of) the monitoring on the access policy.
  - A link between the access of medical records and whether there is a treatment relationship

Access policy is not adhered by the staff

- *Number of participants that named the risk: 2*

- Manifests:
  - User uses the system with the account of a colleague – not a big risk short term, but could have major consequences in the long term
  - User needs more access privileges, which takes about 2 days
  - User with many privileges (e.g. on-call service staff) give themselves more privileges
  - Someone that is not a (full-time) staff member needs access to the system. For example:

    * Person that comes in once a month to conduct checks
    * Freelancer/self-employed person (zzp'er)
  - Staff member goes to another department
  - Staff member does not have the correct privileges
  - Staff role is hard to define and give the right permissions in Epic (not sure if I should include)

- Example:

  - User does not receive access privileges on time
  - Staff member did not complete training on time but does need access to the system and thus uses the account of a colleague
  - Staff member needs more privileges to provide support (so give themselves more privileges)
  - Manager forgets to requests access privileges for a new staff member and/or to register them in for a training
  - Staff member is logged into a shared computer that other colleagues also use
    * For example in a surgery room, where it's also not safe nor convenient to constantly log in and out
  - Interns (coschappen) go to different departments during their internship. They may not have access to the right documents on the first few days as they are still under their previous department in the system. To view the files, they will look at medical records with a doctor that does have access.
  - Staff member does not have the correct access privileges: a doctor in training or a basic doctor (meaning they are not a medical specialist). They may work for multiple specialists.

- Prevention:

  - Acceptance. It will happen, no matter how much they try to prevent it.
  - Regular checks of users with extra privileges and possibly retract some of them if they are deemed unnecessary for their function.
  - Discussing with the departments what is possible for prevention.
  - Spreading more awareness that managers need to request access privileges and register their new employees for an Epic training
  - Break-the-glass procedure: you have to state a reason to before being able to access a medical record of a patient with which you don't have a treatment relationship

- Consequences:

  - Medical error is not traceable in the system to whom made the decision that led to the error

- Needed to improve:

  - Ability to give access privileges on the day they are requested (in case the manager forgot to request them)
  - Adjust the progress such that a new staff member automatically gets rights to Epic
  - Better train the managers to know that they have to request access privileges for Epic for new team members and register them for an Epic training.

- Other risks:
  - Compliance compromised
  - Logging is incorrect

Ill-intentioned staff member

- *Number of participants that named the risk: 2*
- How it manifests:
  - Staff member with extensive privileges intentionally puts ransomware or malware on the network
  - Staff member with extensive privileges intentionally damages system (which is easier and less detectable as they have more privileges)
  - Staff member shares information with outsiders
- Has it happened: no.
- Example:
  - Staff member also works for the Chinese or Russian government, and they might be interested in the hospital data
  - Criminal organizations have interest in the hospital and either get someone in the hospital or convince a staff member
- Prevention:
  - Epic made it difficult to export large data files from the system, only people with a reporting role can do this now.
  - You can build reports in Epic, which makes it unnecessary to export large files from the system
- Consequence:
  - Data breach
- Needed to improve:
  - More extensive screening of potential new staff members (more than the VOG)
- Other risks:

  - Data breach
  - Malware installed
  - Integrity of system
  - Availability of system

Unauthorized access to programs (by users)

- *Number of participants that named the risk: 2*
- Explanation: Manager has to report if an employee leaves to HR and HR reports this to ICT and functional management. Then access will be revoked for the former employee (in one of the hospitals).
- How it manifests:
  - Weak passwords
  - No unique person/real staff member is linked to an account
  - Admin password is known among more than 1 person
    - As it is a highly privileged account, multiple staff members have access/-know the password of it (out of necessity). Therefore it is unclear who uses the account
  - Admins can commit identity theft by overwriting part of the access security of Epic and then using the account of another staff member.
  - Access privileges are assigned to the wrong user account
  - Accessibility service accounts (which have extensive privileges) are misused
  - Employee that has left may still have access to Epic
- Example:
  - Member of the administration team gets the privileges of a doctor
  - On-call accounts need to be able to help, and therefore have extensive privileges
- Prevention:
  - Strict controls of activity on admin account
  - Same password policy for all systems, which prevents the use of weak passwords
  - Twice a year check if all staff members with access to the system are still part of the hospital staff
  - Paying extra attention to staff members that have extensive privileges.
  - If people leave as employee, their wide access to the systems is revoked on the day they leave.
- Consequences:
  - Fraud
    - Going by the first example, the staff member could say they have conducted a consult (which they did not), which will then be invoiced to the health insurance of the patient
  - Patient privacy may be violated

Account that are not linked to a (single) staff member/person-specific

- How it manifests
  - Admin account has multiple user
  - People that are not part of the staff may need temporary access to the system, and therefore there is a separate account that can be used for this purpose.
- Example:
  - Account for patients that need a transplant
    - This happens fast, and can be done by a medical team that is from another hospital. However, this team will need access to the system.

E.3 Continuity

Availability of the system and the medical records

- *Number of participants that named the risk: 3*
- **P2:** one of the highest priority risks
- How it manifests:
  - Hacker
  - During an upgrade
  - Other software supplies data to Epic, and this software gives an error
  - Operations are extended past the normal times, due to which the system still needs to be live (it is down while updating)
  - Outdated IT
- Example:
  - Video call with patient does not work
  - Patient portal does not work
  - Computer that end user uses for work
  - Power outage (very low risk)
  - Flooding
- Prevention:
  - Live copy in another data center
  - Computers with a separate power supply and back-up
  - Good infrastructure (data center, electricity)
    - In America, the hospitals are bigger and they have more problems with infrastructure (power cables have to go longer distances and data centers are further away). Therefore, we have less problems in the Netherlands with the system not being available and the Dutch hospitals make a distorted picture of the struggles with availability around the world.

  - Epic in read-only copies available *(mentioned by 2 participants)*
  - Testing of power supply
  - Testing of network
  - A lot of resources are put towards preventing this risk from happening
  - Extra hard drives, such that the system can handle some hard drives malfunctioning or not being available
  - Server and data are stored in different data centers, with different power supplies and batteries.
  - Redundant internet connection to the hospital, where the cable is also made of high quality material.
  - Testing of the emergency power supply once a year.

- Actions taken if it happens: Crisis management team gathers and determines impact on the provision of healthcare (which meetings and treatments can happen and which can't)

- Consequences:

  - Chain dependence on all the software that communicate with Epic
  - Worst case: medical care has to be halted and/or delayed
    * Sending patients home
    * Stopping or delaying operations
    * Cancelling appointments
  - Medical records are not available *(mentioned by 2 participants)*
  - If it's down for 20 minutes, patients will likely have to be send home
  - Costs the hospital money (as they can't treat patients)
  - Worst case: hospital is offline.
  - Staff is unaware of what to when Epic is offline

- Needed to improve:

  - Time, there is a big workload so people don't have time to make themselves knowledgeable.
  - More communication to make people aware of what they can do if Epic does go offline
  - More awareness among staff about the possibility of the system not being available
    * The system actually not being available, as people are not aware and not worried that it can happen, as it has not happened before

Power failure

Network is no longer available

- Prevention:
  - Back-up computers
- Actions taken:
  - Crisis team
- Consequences:
  - Epic is unavailable

E.4 Cyber security

Old hardware

- When it manifests:
  - Staff uses old laptops to access the system
  - Not enough budget to replace hardware
  - Operating system on devices that connect is outdated/not the newest version. For example it's not running on the newest Windows version.
  - They don't take into consideration all the aspects that it takes to access Epic, which results in budget going to things that are less important to the core business and important causes not receiving any budget.
- Example:
  - Computer shuts down and staff member cannot work for half-an-hour or until they get a replacement.
  - A lot of aspects of Epic are redundant (i.e. the network connection and power supply). They therefore conclude that Epic is always available for staff members. However, it is not taken into consideration that the staff members may have old devices that have a higher probability of shutting down or being hacked, which would make Epic unavailable to them and compromise the system.

Patient information is saved outside of Epic/hospital systems

- How it manifests:
  - Data is saved in a mail, network drive, personal drive or USB for example.
  - Using a CD ROM or DVD to send scans to other hospitals
  - Staff feels that they don't have an alternative (other than using for example mail), or that the alternative is insufficient, and therefore saves and/or sends data outside of Epic.

- Example:
  - Usage of project management tools such as Trello
- Prevention:
  - USB portals have been disabled in all devices. However, this is not foolproof and the participant does think there may be some hospital data on a USB.
  - Sending data to other hospitals via a secured network
  - Offering a compliant alternative to staff, as everyone wants to do it the right way to deliver the highest quality of care. They just feel like the current software is insufficient.
- Actions taken when it happens:
  - Team is addressed on saving data outside of the system, and is informed of which information cannot be uploaded or otherwise used or processed there.
- Consequence:
  - Breach of confidentiality
  - Information on hard drives/locations that it is not supposed to be
- Needed to do better:
  - A good alternative to save data, so staff doesn't feel the need to safe information outside of the system

Security of the patient portal

- Examples:
  - Cookies are not flagged.
  - Multifactor authentication
- Prevention:
  - Strict monitoring
  - Epic has a policy regarding Microsoft Patching, in which they test their system within a week that a patch is released
  - Hospital checks Microsoft patches.
  - Audits
  - Their prevention means that they don't have risks
  - Epic forces the use of the most recent version
  - Epic quickly solves security issues, also if you address them
  - Two factor authentication
  - Using of external parties for security

  - Ethical hackers
  - Constant scans of the network
  - VM Microsoft Defender for Endpoint.
  - Yearly pen tests.

Data breach (hacker gains access to system)

- *Number of participants that named the risk: 2*
- How it manifests:
  - Hacker uses user credentials to access system (password hacking)
  - New publication of the patient portal.
  - Mobile applications that staff use to enter the system from home or from a patients home.
  - PC's/laptops are not locked
  - Staff members don't use two factor identification
  - Staff members download malware (by accident)
- Example:
  - With 2 factor authentication, the user gets spammed with requests if they're trying to log in until they accept
  - Staff member opens/downloads things for personal use that contain malware on a device connected to Epic
  - Word document that user has for personal use in which they fill in confidential information
- Responsible for it: security team, CISO.
- Did it happen?: Not within Epic
- Prevention:
  - For 2 factor authentication you now need to give the 2 numbers that are on your computer screen to give access, this way users cannot just click on 'yes' when they're getting spammed
  - Logging of access to data
  - Application to exchange data with different software (creating a safe data transportation method)
  - Hotline for data breaches
  - Parts of the system that are shared outside of the hospital (for example with third parties) are read-only
  - Constant trying to detect data leaks.
  - Logging the system
  - Awareness campaigns.

- Actions taken when it happens:
  - Hotline is called and starts investigating the data breach (which data is found, where did it happen, how did it happen, who is affected).
- Needed to improve:
  - More awareness among end-users
- Other risks:
  - Integrity of system is compromised
  - Privacy of patients is compromised
  - System may be unavailable

Cyber security attack

Malware

- **P3:** biggest threat
- How it manifests:
  - Malware is in your network for a long time before it activates/damages the system
  - User downloads malware
  - DDoS attack
- Example:
  - DDoS attack
  - Virus applications found on the network
  - See data breach risk example
- Did it happen?: Virus applications have been found, but they did not encrypt any data
- Prevention:
  - Back-up system
  - Testing of back-ups
  - Immutable back-ups (you can't adjust them anymore after they've been made)
  - Logging of access to data
- Actions taken when it happens:
  - If a virus application is found on a device, the device is investigated and cleaned before it is allowed to connect to the network again.

- Consequences:
  - Data (medical records) will be lost if a back-up needs to be used. Due to the large system, there are no back-ups for longer than a month.
  - Data may be encrypted by the hacker
- Needed to improve:
  - More budget, for example to have a back-up in the cloud
- Other risks:
  - System not available

Ransomware

- *Number of participants that named the risk: 2*
- **P1 & P4:** named this is a high priority risk
- Consequences: confidentiality, integrity and availability system is compromised.

E.5 Change Management

Releases/updates can not go live

- How it manifests:
  - Operations are extended past the normal times, due to which the system still needs to be live (it is down while updating)
  - Knowledge is missing in order to fully test the upgraded version

Changes have unexpected impact

- *Number of participants that named the risk: 3*
- **P4:** biggest risk within change management
- How it manifests:
  - Changes made by the hospital (standalone changes)
    - Impact of changes was misjudged
    - Not enough knowledge available to judge the impact of a change
    - Insufficient testing of changes
    - Implemented changes are recorded in different tools
    - Teams implement their own vision on how to make changes, even though there is an overall process in place
    - Hard to get a full overview and control over all the changes that are made
  - Upgrade of Epic that causes an error with the way the hospital build Epic *(Mentioned by 2 participants)*

  - Large and complex system
  - No data model of the system

- Has it happened?: no
- How often it happens: not often
- Example:
  - New medication that needs to be added to the medication list
  - New dosage of medication needs to be added to the medication list
  - New way of medicine intake
  - Changing forms (to e.g. request medication)
  - Users with a specific role cannot see a button (due to their access settings)
  - Functionality is temporary disabled, as they did not notice it was disabled. For example a data point is not processed in a report
- Prevention:
  - Epic upgrades are well thought out
  - Ensure that staff member knows what impact their changes have (which is difficult)
  - Progress for requesting changes
  - Quick response time to solve the issue
  - Raising awareness among developers that this can happen
  - Several test and control procedures in place before a change is live
  - Copy of the live version every day, on which new functionalities can be tested
- Consequences:
  - Change causes an error or malfunction
    - Other parts of the system don't work well/anymore
    - UI may not show something correctly anymore or incorrectly
  - Extra work as they have to change the current live Epic version to a previous version
  - Often is something small
  - Obstruction of patient care
- What is needed to improve:
  - A standard progress to request changes for all teams
  - A data model
- Other risks:
  - Continuity (or obstruction) of patient care
  - Integrity of system (it is compromised by changes in the system, due to which the hospital can't be sure if the information in Epic is correct)

Black box

- How it manifests:
  - No data model of the system
  - System is very large
- Consequences:
  - It is not clear what impact changes to the system have (changes that are made by the hospital)
  - Hospital is dependent on expert opinions to check what impact a change may have
  - Changes have an unexpected impact
- Prevention
  - Epic already provides a lot of support and tools in order to work with the system
- Other risks:
  - Dependence on experts
  - Changes have an unexpected impact

Old base of the system

- How it manifests:
  - Epic still uses techniques from the '70.
- Consequences:
  - Hospital needs to use outdated techniques in order to update system, which new staff members may not be familiar with.

Large size of the system

- How it manifests:
  - Hospitals do not use the full system because they cannot (e.g. due to time limitations) implement the whole system
  - Hospital can differ a lot from the foundation of the Epic system
  - Changes can have unforeseen impacts (see black box consequences)
- Consequence:
  - Investment in system is not fully utilized
  - Hospital staff in charge of the system needs to explain to other (like the board) why the hospital is not using the full system

- Prevention:
  - Epic has a rating in which the hospital can view how much of the system they have implemented, in order to motivate them to implement the full system
- Other risks:
  - Dependence on experts
  - Changes have unforeseen impacts

Missing overview of the full system

- *Number of participants that named the risk: 2*
- How it manifests:
  - Changes are not documented well/correctly
  - If your ticketing system is not linked to Epic, you can't view the changes.
  - The system is very customizable, and many departments change the modules they work with to fit their needs
  - Customizability of Epic
  - Each hospital that uses Epic has a different foundation
  - Hospital builds features that they can use for themselves
- Consequence:
  - Many hospitals build the same feature, but because they have a different foundations they cannot build it together or share it, resulting in both hospitals investing a lot more time, costs and resources than if this was possible
  - IT department does not have a clear view of how the system works and which features are activated and used
  - Labor-intensive to check all the changes and verify that they will work (i.e. do an impact analysis)
- Other risks:
  - Quality of system may degrade due to the many changes
- Prevention:
  - Change management protocols

Dependence on expert opinions, difficulty securing knowledge

- How it manifests:
  - Takes 6 months to get a certification in order to work with the system, and another 6 months to become familiar with the system
  - System is large and complex, which makes it difficult to become familiar with the system
  - High turn-over rate
- Consequence:
  - More dependence on senior/small group of staff members to secure knowledge
- Prevention:
  - Epic customer service is always reachable and prepared to help, which allows the hospital to solve knowledge gaps

Upgrades from Epic that may cause a crash

- Prevention:
  - Updates only done in the evening/night
  - Staff is informed of when the system is not available (due to updating the system)
  - Lots of testing of upgrades

E.6 Supplier Management

Different laws and regulations in America vs Netherlands

- *Number of participants that named the risk: 2*
- How it manifests:
  - Epic may not be allowed access to all the data by Dutch law
  - Difference in insights and priorities of hospital and Epic
  - Epic offers a functionality that is not allowed in the Netherlands
- Example:
  - Epic adds information in the patient portal, that the patient can see, which they are not allowed to see in the Netherlands
  - Extra requirements form the Dutch government in order for patients to be able to log into the patient portal with their DigiD
- Consequence:

  - Extra work for the hospital in order to comply with Dutch laws.
  - Extra costs as Epic requires payment in order to adjust their software to comply to Dutch laws
  - Hospital needs to make a consideration between paying extra costs and how to fully comply with the Dutch regulations.
  - Worst case: new release has to be postponed

- Other risks:
  - Tensions with Epic when a feature does not comply with the Dutch laws and regulations, but Epic does push to implement the update
  - Tensions in the hospital as they may need to work extra hours to make a release deadline and ensure Epic complies with Dutch laws and regulations.

- Prevention:
  - Hospitals checks if they have the right security measures to comply with the Dutch laws
  - Privacy contract
  - Epic gives monthly reports to their clients informing them of the laws and regulations applicable in the country of the client.
  - If functionality is illegal, Epic can provide a work-around with no extra costs for the hospital

Epic system is expensive

Third party management

- How it manifests:
  - Third parties that work with the hospital can be critical of Epic and if they will fulfill their promises based on their own experiences with suppliers.

Bugs in the system

- Prevention:
  - Regular updates by Epic (4 per year)
  - Weekly security check
  - Thorough testing of new releases

Trustworthiness of Epic

- How it manifests:
  - During acquisition of a new EHR system
  - Epic is privately held and the owner of Epic has a lot of influence on the product and the vision of the company. If the company switches owner the vision may also change – this was marked as a low risk

- Prevention:
  - Check if other hospitals may be using this EHR system
  - Look at the track record of the company
  - Arrange external audits for Epic
  - Operational testing
  - Establishing trust through working with them