Master Degree Project

ISMS and privacy challenges related to PeHS:

A Qualitative study

Emelie Mannebäck

Supervisor: Ali Padyab
Examiner: Rose-Mharie Åhlfeldt

Master Degree Project (120 ECTS) in Informatics
with a specialization in
Privacy, Information and Cybersecurity
30 ECTS
Spring term 2022

ACKNOWLEDGEMENTS

First, I would like to express my gratitude to Rose-Mharie Åhlfeldt for approaching me with the idea of this thesis project and for the invitation to collaborate with the research consortium DOME. Your help and guidance throughout the project and access to the resources from DOME work were greatly appreciated.

I would also like to thank my thesis supervisor Ali Padyab for the continuous support and guidance throughout project. Your confidence in my work assured me along the way and pushed me to raise the ambition level even higher.

ABSTRACT

The future of healthcare is increasingly digital, which includes a shift towards more personalised services that allow for more patient-centred and transparent patient care. These services are defined as PeHS and although there are great potential benefits of these services, there are also challenges regarding information security and privacy related to providing this type of services. This thesis project aims to examine the state of ISMS related to PeHS, which would also involve an examination of considerations taken regarding privacy in PeHS.

The data collection methods for this thesis project were a systematic literature review and qualitative interviews. In total 18,667 publications published between 2017 and 2022 were found during the database searches. When the selection criteria had been applied 17 publications from the search process and 1 publication from the backward snowball process were accepted. The accepted publications were analysed by applying thematic analysis. Furthermore, two interviews with three participants were conducted after the literature review had been completed. The interview material was analysed by applying the analysis method of qualitative content analysis.

The results showed that there are several challenges regarding ISMS and privacy related to PeHS. For example, there is a lack of knowledge within the organisations on why they should be applying the methods and tools available to ensure the security of the information flow through the healthcare services. Another example is the challenge of keeping up with the pace of digitalisation and adjust the ISMS to ensure sufficient information security of the services.

Keywords: ISMS, privacy, Personal eHealth Services, PeHS

Table of Contents

1. Introduction

In this digital age organisations of all sizes handle extensive amounts of sensitive and valuable information, and they must apply a variety of technology and administrative measures to uphold an optimal level of security for that information (Isaksson & Sanne, 2006). The future of healthcare is also increasingly digital and by transitioning to digital healthcare a shift in focus to more personalised services in which e-services are applied is possible, which will allow for more patient-centred and transparent patient care. These services are often web-based and can be used by patients to read their Electronic Health Records (EHR), and when this is allowed the records are referred to as Patient Accessible Electronic Health Records (PAEHR) (Nurgalieva et al., 2020; Sahama et al., 2013).

The Swedish Patient Data Act (2008:355) states that patients must have access to their care and treatment information to be able to actively participate in their own healthcare. Moreover, the Swedish National Regulatory Framework (NRF) requires that citizens should have access to their digital health information (Scandurra et al., 2017). Thus, all healthcare regions within Sweden have recognised the NRF and it was decided that by the year 2017 should all Swedish citizens have access to their available digital health data through a national eHealth service (Scandurra et al., 2015). Therefore, Swedish citizens can gain access to their PAEHR through the online portal Journalen (*Journalen - Inera*, 2022), through which they have access to information varying from lab results to open notes written by their physician regarding their care (Bärkås et al., 2021; Nurgalieva et al., 2020). This has improved the potential of patients to both better understand the healthcare information given to them and increased the usability of the information (Nurgalieva et al., 2020).

A concept related to this is eHealth, which can generally be described as the application of information and communication technologies applied to deliver healthcare services such as communication, sharing, retention and disposal of health information (Sahama et al., 2013). Patient portals, such as Journalen, are eHealth systems that make personal health records accessible by patients and also allow for communication with connected health service providers (Nurgalieva et al., 2020). For example, when logging onto Journalen it is possible for the patient to overview which clinics he is listed at and book appointments directly with them online. Moreover, these portals also allow for healthcare information exchange between care providers (Nurgalieva et al., 2020; Sahama et al., 2013).

Although there are great potential benefits of using EHR and allowing for PAEHR, there are challenges regarding information security and privacy when establishing such systems (Sahama et al., 2013). For example, there are privacy concerns related to identity theft, data falsification, ownership and management of the stored data (Entzeridou et al., 2018). Also, there are information security threats regarding the interaction between the users and the information systems, which relate to applied policies and practices regarding information management (Sahama et al., 2013). As Nurgalieva et al. (2020, p. 2555) stated "*a premise for storing healthcare information digitally in patient portals is keeping it secure*". With shared e-access to PAEHR can the partnership between caregivers

be enhanced and lead to better patient care, but it also introduces privacy and security issues (Nurgalieva et al., 2020). Muendo (2014, p. 1) further explained this by stating "*organisations today transact in a worldwide setting which enables them to work in partnership and share information resources with one another but conversely exposes them to many threats both within and without the organisation, thus the need to secure their information assets*". So, it is possible to say that the more a region's health sector has been able to digitise its processes and services, the more threats and damage can be done to the healthcare infrastructure by targeting the eHealth infrastructure (European Union Agency for Cybersecurity (EU body or agency) et al., 2015).

When dealing with shared health records that can be consulted at any time or location, there are increased threats to confidentiality and the use of eHealth services opens up discussions on controversial areas such as patient privacy (Mohammad & Stergioulas, 2010). As Nurgalieva et al. (2020) emphasised, with an increased information flow in healthcare there is an increased risk of security events occurring and with that there must be an effort made to minimise the risk of those security events. The concept 'privacy' does not have a clear-cut definition because it is being valued based on culturally dependent variables. Since health information is regarded as particularly sensitive, in the context of EHR the first privacy concern is the ability of the individual to control their personal data that is managed by other parties. This is also referred to as 'information privacy' (Sahama et al., 2013).

To secure the process of sharing health records information management that emphasises information security as the core security aspect must be applied, which will help effectively adopt information technology and information sharing (Mohammad & Stergioulas, 2010). As Mohammad & Stergioulas (2010, p. 3919) state "*the concept of information security encompasses some issues like privacy and trust*". Moreover, information security involves areas of integrity, confidentiality, access control, availability, authenticity and utility (Mohammad & Stergioulas, 2010). These increased security demands relate to two aspects of consideration: the information management through policies and practice, and the education, training and awareness of all stakeholders in the security implications of potential events (Sahama et al., 2013).

To provide better knowledge into how to implement PAEHR, an international project NORDeHEALTH has been focused on such eHealth services and to ensure that the digitisation of healthcare truly benefits the different parties involved. The goal of that project is e.g., to shed light on how health information is collected, shared, and used (Hägglund, 2021). This thesis project will be part of work package 5 within a larger research project conducted by DOME, as part of the NORDeHEALTH consortium. The project has been divided into several work packages which in turn focus on e.g., socio-technical contexts or information security related to Personal eHealth Services (PeHS). The goal of work package 5 includes the completion of an analysis of the information security and privacy perspectives related to PeHS. The involved parties in the project are participants from Uppsala University, Örebro University, University of Skövde, Tallinn University of Technology, Aalto University, Karlstad University, Norwegian Centre for E-health Research and OpenNotes (US) (*DOME*, 2022; *NORDeHEALTH*, 2022).

To ensure a greater likelihood of discovering relevant information about the research topic the thesis project has been conducted through the application of a systematic literature review. Several database resources have been utilised by applying a variation of search terms that were deemed appropriate to the topic. To further ensure that the relevant publications were taken into consideration for the review backward snowballing was applied. When the defined selection criteria were applied the process resulted in a bibliography of accepted publications, which were analysed by applying analysis method qualitative content analysis. Moreover, semi-structured interviews were applied to gather the perspective of practitioners on the topic of information security and privacy challenges when providing PeHS to citizens.

1.1 Problem Definition

Smart healthcare services or eHealth are the cause of both positive and negative effects. On the one hand they can facilitate a more sustainable healthcare, but on the other hand they also generate concerns related to information security and privacy (Amankona et al., 2021; Vithanwattana et al., 2021). Moreover, sharing health information electronically between one healthcare giver (or party) and another has been described by several researchers as problematic, both in relation to privacy and information security. For one, by sharing health information the flow of personal and sensitive information increases. Also, the ever-growing risk of threat actors such as hackers deploying attacks (e.g. network hijacking and eavesdropping) can cause major issues for the different parties involved in the information sharing chain (Amankona et al., 2021; Shen et al., 2019; Vithanwattana et al., 2021).

In short, the success of PeHS and eHealth as a whole is completely dependent on the information being accessible in an easy and secure manner (Chowdhury & Ray, 2007). The choice of communication channel is vital when designing PeHS since unsecured channels could allow for unauthorised disclosure of personal information. Therefore, when discussing eHealth one must consider how the information is going to be accessed, processed, stored and transferred, both from the perspective of privacy and information security (Amankona et al., 2021; Gajanayake et al., 2011).

For some years, implementation of Personal eHealth services has been carried out internationally and plenty of resources have been designated to do so. Although, contextual factors have not been taken into consideration as of yet on an appropriate level (*DOME*, 2022). For example, there is still a lack of insight into the contextual differences with PeHS, which includes what policies have been applied and the level of accessibility (Hägglund, 2021). Yet, in the literature there is a knowledge gap into what the challenges of ISMS and privacy are more precisely in relation to PeHS.

1.2 Aim and Purpose

Reflecting upon the research problem presented above and the research conducted by DOME, the purpose of this thesis project is to understand and describe the issues related to ISMS and privacy regarding the use of PeHS. This thesis project aims to examine the state of ISMS related to PeHS, which would also involve an examination of considerations taken regarding privacy in PeHS. Moreover, the aim also includes an examination of how practitioners are working with ISMS and privacy concerns concerning their PeHS.

1.3 Research Questions

The two research questions for the thesis project are:

1. What are the challenges with ISMS and privacy in relation to PeHS?
2. How are Swedish regions applying ISMS for their PeHS and how are they managing the privacy concerns regarding PeHS?

1.4 Delimitations

The intention of this thesis project is not to provide any solution formulation to the challenges found regarding ISMS and privacy in relation to PeHS. Nor technical challenges regarding for example, technical setup. Moreover, it is not intended to provide the involved interview participants with an extensive list of success factors or challenges in PeHS, but to probe them based on the challenges found in scientific literature.

The following is an overview of the remaining structure of the thesis report: Chapter 2 will present the background to the thesis work, including four main concepts and relevant standards, and provides insight into existing research done within the area. The research methodology is presented in chapter 3. This includes a description of the research approach, the planning of the systematic literature review and qualitative interviews. The chapter also presents the data analysis methods thematic analysis and qualitative content analysis. Chapter 3 ends with an explanation of ethical considerations taken and how threats to validity have been managed. Chapter 4 is dedicated to presenting the practical application of all the involved methods, both for data collection and data analysis. The results for both the systematic literature review and the qualitative interviews are presented individually and jointly, in chapter 5. The discussions on previous research, methods, application, results, ethical and societal aspects are provided in chapter 6. Chapter 7 is the final chapter of this thesis report, and it presents the conclusions drawn from the literature review and qualitative interviews while also presenting recommendations for future work in the research area.

2. Background

This chapter provides a background to the research area of the thesis work. Firstly, the main concepts related to the study are described. Secondly, related works are presented to provide insight into previous research done within this area.

2.1 Main concepts

There are four main concepts related to the thesis work: ISMS, PeHS, patient privacy and cybersecurity. Moreover, there are four ISO standards to take into consideration concerning the research area: ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27701 and ISO/IEC 27799. These concepts and standards are explained below.

2.1.1 Information Security Management System

Information security can be described as the protection of information by ensuring the three areas of confidentiality, integrity and availability (*ISO/IEC 27000*, 2018; von Solms & van Niekerk, 2013). Confidentiality has been defined by ISO/IEC 27000:2018 (2018, p. 2) as "*property that information is not made available or disclosed to unauthorised individuals, entities, or processes*". Furthermore, the definition of availability is found to be "*property of being accessible and usable on demand by an authorised entity*" (*ISO/IEC 27000*, 2018, p. 2). Lastly, integrity is defined by ISO/IEC 27000:2018 (p. 5) as the "*property of accuracy and completeness*". Moreover, information security encompasses any system or hardware that either use, store or transmit the information in question (Whitman & Mattord, 2014) and involves the application and administration of proper controls to manage threats to business success and continuity (*ISO/IEC 27000*, 2018). At the core of information security, there are the users, the human element, which through their behaviour and interaction with the information and information systems can critically affect the information security effect (Muendo, 2014). As described by Reid & Van Niekerk (2014), the users (including caregivers, patients etc.) of information and information systems can become a threat to the applied information security solution and are therefore the weakest link in the information security chain.

Moreover, an information security management system (ISMS) includes the implementation and management of policies, processes, procedures, organisational structures, software, and hardware to protect the information assets (*ISO/IEC 27000*, 2018). Wawak (2012, p. 42) describes the scope of ISMS as "*the development of the security policy at the strategic level, the evaluation of the risks relating to threat occurrence, the determination and implementation of security controls aimed at eliminating such threats, and also the monitoring of the systems with the aid of internal audits and a management review*".

The Swedish Civil Contingencies Agency (MSB) provides guidance for implementing an ISMS, which is based on the standards ISO/IEC 27001:2017 and ISO/IEC 270012. MSB has divided the implementation process of ISMS into four phases, which is visualised in Figure 1 (MSB, 2018):

A. Plan – Identify and analyse

The first phase is known as the establishment phase in which the ISMS policy, scope and boundaries are defined through analysing the internal organisation and the external environment. This requires great knowledge about the organisation and the information that is managed within the organisation. To gather this knowledge documents can be collected, discussions and workshops should also be conducted. The results from this phase are internal and external prerequisites and how they affect the information security work.

B. Do - Implement and operate

In the second phase, the ISMS is implemented through the design of a risk mitigation plan and an assessment plan, implementation of controls and training programs etc. This phase also includes the design of an annual management plan for information security specifically.

C. Check - Maintain and improve

It is in the third phase that the previous activities are realised and used. This requires effort put into both training and communication throughout the organisation. Moreover, the process performance of the ISMS policy is assessed to identify points of improvement.

D. Act - Monitor and review

The last step of the ISMS process includes actions to achieve constant improvement of the management process. This means that there is no actual 'end' to the ISMS process. Instead, it is circular. In this phase points of improvement should be identified and implemented, and changes made should be communicated with affected stakeholders. In short, this phase provides guidance on the evaluation of the information security work and its management. The results from this phase should make up the material used for internal reviews, management review and as input to the next iteration of the systematic information security work.

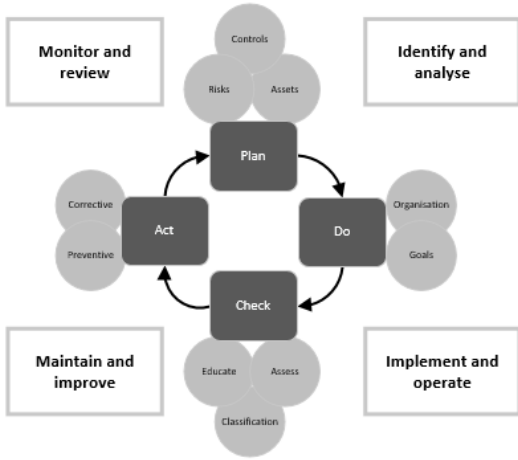

Figure 1. Information Security Management System process

An important point to note regarding ISMS is that it is paramount that clear boundaries and scope are defined in which the ISMS is supposed to be applied. Both the business environment and the Internet are huge and diverse areas on their own, therefore the organisation or responsible party for the ISMS process must determine where to draw a line between what counts as within the organisation and what is without. In short, the boundaries must be physically or logically identifiable. The boundaries are defined in terms of the organisation that is to be safeguarded, including which networks and data, and at which geographic locations (Calder et al., 2019).

2.1.2 Personal eHealth Services

The concept of eHealth can be exemplified with the transition from prescriptions being written on paper to prescriptions being accessible, managed and prescribed online. Or the use of Electronic Health Record instead of traditional paper charts. The function of allowing patients or caregivers to book appointments online is also an example of eHealth (E-hälsomyndigheten, 2019). When citizens are given access to their EHR it is usually done through web-based portals, and it is then referred to as Patient Accessible Electronic Health Records. The phenomena of these patient accessible portals have become quite widespread internationally, but they and the functions they offer are not the standard (Bärkås et al., 2021).

There are three categories of eHealth: communication, availability, and organisation. Communication emphasises that eHealth is beneficial for improving the communication between caregivers (personnel, hospitals, clinics etc.) and patients. Moreover, availability is focused on the ability to allow patients to be more involved and actively participate in their care by being able to e.g., book appointments with their caregivers online. Lastly, the category organisation implies that eHealth provides tools for healthcare that e.g., allows healthcare personnel to more quickly get hold of relevant and important information which in turn improves the effectiveness of the healthcare (E-hälsomyndigheten, 2019).

Moreover, eHealth services are provided to citizens that will allow them to monitor, manage and document their own health information, either for their own sake or for the purpose of sharing it with their physician (Erlingsdottir & Sandberg, 2019). These Personal eHealth Services provide a set of important functions, a way of storage, and secure, reliable, and instant communication between each individual and the public health service (Burkow et al., 2008). Since these eHealth services depend on the sensitive personal health data of citizens, actions must be taken to implement appropriate access controls to ensure that private health information is safeguarded. This for example means that not all physicians or other eHealth service providers can gain access to the information by default (Widmer et al., 2013).

2.1.3 Patient privacy

The concept ‘patient privacy’ is both complex and heavy due to differing values on the topic of privacy. The concept is constantly evolving due to the balancing act between safeguarding the privacy of the patient against the need for patient data (Shen et al., 2019). In a paper by Åhlfeldt & Söderström (2007) participants predicted that in the future patient privacy would be at risk because of issues related to administrative security. Worries concerning the continuous increase

of information being generated and transferred were also communicated, especially the fear of the weakest link in the security chain remaining which is the individual employee. Moreover, in an article in the Swedish medical journal from 2005 (Sjödin, 2005) concerns regarding the use of medical records being registered and shared throughout the healthcare chain were expressed, both from the physicians‘ and the patients’ perspectives. Therefore, to maintain patient privacy, permission to relevant patient information must be given depending on the healthcare actors’ need and not be given out without control (Åhlfeldt & Söderström, 2007).

A recent study by Ak et al. (2021) found that the perspective of privacy can be affected by conditions such as gender and culture. Furthermore, it was found that privacy most closely relates to confidentiality and should be considered for all types of patient information. The difficult balance between patient privacy and need for patient data is distinct within healthcare, especially due to the sector becoming more integrated and the increasing requirements of being able to follow the patient’s interactions with the healthcare actors since they collaborate in the patient care.

2.1.4 Cybersecurity

Since PeHS are integrated into the healthcare’s network and eHealth infrastructure a concept to take into consideration is cybersecurity, which can be defined as the organisation and collection of resources, processes and structures applied to safeguard cyberspace and systems allowed in cyberspace from events that deviate from property rights (Craigen et al., 2014; Eugen & Petru, 2018).

Moreover, cybersecurity does not solely concern the protection of cyberspace itself, it also involves the protection of possible information assets that could be reached through cyberspace. This ultimately implies that when assets are accessible through cyberspace information security and cybersecurity intersect (von Solms & van Niekerk, 2013). Eugen & Petru (2018, p. 360) go one step further by stating “*in addition to technology, cybersecurity also refers to the fact that people have access to data and processes involved*”.

Patient information is highly valuable and sensitive, and attacks on getting a hold of such data have increased during the Covid-19 pandemic (Marshal et al., 2021). Earlier statistics showed that financial services were the highest at-risk industry up until 2015, then the healthcare industry became the top target for cyber-attacks. It was found that in 100 different countries a stunning 100 million health records were breached in 2015 (Alharam & El-medany, 2017).

2.1.5 Related ISO Standards

The purpose of standards is to provide guidelines into how to safeguard an organisation’s information assets from the perspective of confidentiality, integrity, and availability. The standards do not, therefore, provide a ‘one solution fits all situations’ solution, instead, they provide guidance and frameworks. Moreover, this ultimately means that the success of the standards is reliant on the organisation’s own risk assessment and understanding of the standards (Alfawaz, 2011).

There are several well-established standards within the area of information security management and information security management systems, which in short are often referred to as the ISO 27000-series (Haufe et al., 2016). With this thesis work, four ISO standards are regarded as highly relevant: ISO/IEC 27001:2017, ISO/IEC 27002:2022, ISO/IEC 27701:2021 and ISO 27799:2016.

ISO/IEC 27001

This standard is the second one in the ISO 27000- series and is focused on information security management. This standard provides general guidance and approaches for risk management. Simply put, ISO/IEC 27001 specifies the requirements for a functional ISMS (Calder et al., 2019). Implementing an ISMS is a strategic decision since the establishment and implementation is directly affected by the needs and objectives, security requirements, organisational processes used, size and structure within the organisation. All of which are evolving (*ISO/IEC 27001*, 2017).

This standard has over the years become more and more important for information security work since it offers a practical solution to the ever-growing range of information-related regulatory requirements. Moreover, it has helped organisations become more cost-effective since they put the resources into the management of possible security threats rather than paying the consequences of those threats. This has also led to a greater number of organisations aiming to get ISO/IEC 27001 certified and such a certification has high recognition globally (Calder et al., 2019). The standard emphasises the absolute need of the ISMS being accepted as part of and integrated with the organisational processes, management structure and that information security is given a prominent role in the design of future processes, information systems, and controls. All of this is possible since the ISMS implementation can and should be scaled according to the organisational needs (*ISO/IEC 27001*, 2017).

ISO/IEC 27002

The next standard in the ISO 27000-series is ISO/IEC 27002 which provides a code of practice and is primarily focused on best-practice guidance of the security controls provided in Annex A of ISO/IEC 27001. In addition, some guidance is included regarding risk assessment (Calder et al., 2019). By utilising this standard, the organisation is assisted in the choice of information security controls in the implementation process of an ISMS. It is therefore required to apply ISO/IEC 27002 in conjunction with the other standards in the ISO 27000-series (*ISO/IEC 27002*, 2022). The relation between ISO/IEC 27000, ISO/IEC 27001 and ISO/IEC 27002 can be described as the following. The overview and overall guidance related to information security management systems including vocabulary is given in ISO/IEC 27000. Moreover, this standard explains and references the other standards within the series with related terms and definitions. ISO/IEC 27001 gets more detailed and is focused on the security techniques and the implementation process of ISMS (*ISO/IEC 27001*, 2017). Lastly, ISO/IEC 27002 is primarily focused on the last step of the ISMS process which is the choice and implementation of information security controls (*ISO/IEC 27002*, 2022). The correlation between the standards of the ISO 27000-series is illustrated in Figure 2.

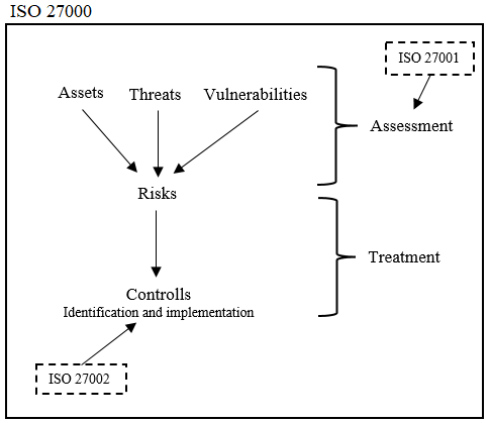

Figure 2. Relationship between ISO standards related to the thesis

ISO/IEC 27701

In relation to privacy there is standard ISO/IEC 277701, which is an extension to ISO/IEC 27001 and ISO/IEC 27002 that deal with privacy information management. This standard is applicable for all types and sizes of organisations that process Personally Identifiable Information (PII), which most organisations do today. This includes public and private companies, government entities and non-profit organisations. Moreover, the quantity and types of PII being processed are increasing. This ultimately puts pressure on privacy protection, which in relation to PII is a worldwide societal need and topic of legislation/regulation. Depending on the organisational context and national legislation or regulation, the requirements and guidance for PII vary and therefore one must understand that this standard is meant to be applied as an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organisation (*ISO/IEC 27701*, 2021).

The ISO/IEC 27701 encourages the organisation to align and integrate its Privacy Information Management System (PIMS) with the requirement of e.g., an ISMS as defined in ISO 27001. Much as the standards in the ISO 27000-series, ISO/IEC 27701 provides guidance to establish, implement, maintain, and continuously improve the PIMS. In other words, the organisation that complies with the requirements in this standard will generate documentary evidence of how it handles the processing of PII (*ISO/IEC 27701*, 2021).

ISO/IEC 27799

Although personal data is generated and managed by many companies, institutions, and authorities there are special requirements on the protection and security of personal data within the healthcare sector. The security of such data is focused on areas such as confidentiality, integrity, and availability, but there is another layer to the security since the data is in direct connection to e.g., patient safety and audibility throughout the life cycle of the data. The protection of this information also relates to patients' privacy. Moreover, information systems within healthcare are required to fulfil unique requirements since healthcare cannot stop even though there might be e.g., natural disasters, system failures or

cyber-attacks. This also requires knowledge of how the health and medical care sector functions (*ISO 27799*, 2016) with all its various information flows (Sari et al., 2021). Especially since personal information is shared electronically within healthcare through the application of e.g., eHealth services, which is why it is beneficial to define a common standpoint for the management of information security in health care. What ISO/IEC 27799 does to help improve the information security in healthcare is to provide guidelines to support the interpretation and implementation in health informatics of standard ISO/IEC 27002 (*ISO 27799*, 2016).

Moreover, what this standard provides is implementation guidance of the information security controls given in ISO/IEC 27002. ISO/IEC 27799 also provides an adaptation of the controls where necessary to better fit the management of health information security. However, it is emphasised that this standard is not meant to replace any of the other standards of the ISO 27000-series. For the standard to be as efficient as possible it has been designed based on the experience of international efforts to ensure the protection of personal data in healthcare and is supposed to be applied as a complement in conjunction with the other standards such as ISO/IEC 27001 and ISO/IEC 27002. Just like organisations from other sectors, healthcare organisations such as a hospital can become ISO/IEC 27001 certified, and that certification does not require any compliance with ISO/IEC 27799. The hope is that there will be stricter requirements in the future and that the standard will become publicly available to improve and ensure the information security of personal information within the healthcare sector (*ISO 27799*, 2016).

2.2 Research background

In a study by Jara & Schafir (2014) the researchers briefly touched upon the challenges to privacy and information security in relation to eHealth available in Latin America. They found that there were issues with privacy due to lacking data encryption, monitoring, and backup process. Moreover, they identified that there were two security requirements in addition to confidentiality, integrity and availability which were authenticity and accountability. Although, this study did not present or cover any challenges in relation to ISMS.

Another study by Mense et al. (2013) looked at the management and exchange of health information from the information security perspective. In this study, the researchers described that the organisations are unfortunately likely to misunderstand the concept of information security as something that mainly requires technical security controls. They emphasised that true information security is a combination of technical and organisational measures. Mense et al. (2013) described the need for a proper ISMS since security requirements are dynamic rather than static. The main challenge they presented was that organisations must define and maintain an organisational framework to appropriately sustain a proper level of security from a cross-organizational information security context. Although, as the researchers themselves state in their conclusion, the results of this study were intermediate and would require further work to include a larger number of ISMS aspects. In addition, this study was limited since it focused on evaluating requirements and defining basic concepts of ISMS (Mense et al., 2013). Therefore, they did not include a privacy perspective in their results.

A study from 2017 stated that the implementation of eHealth services had been limited due to the fact that there was resilience to such developments relating to concerns about security and privacy (Scandurra et al., 2017). Moreover, due to a gap between the legislation at that time and the development of PAEHR questions arose relating to e.g., the ownership of the health information. This was explained by the researchers as the result of healthcare is a complex organisation to manage since several different actors have to collaborate within the same area (Scandurra et al., 2017). Since this study was published, new legislation has been provided e.g., GDPR and healthcare providers have had to adjust their PeHS to meet the new legal requirements.

The recent study by Sari et al. (2021) declared that there is a lack of research into inter-organizational information security management systems. Especially concerning the involvement of the people involved and the organisation design/strategy, which are vital elements to ensure information security. This study was focused on investigating the practices and challenges of information security for IOS in healthcare services from the perspective of a health regulator. Therefore, it did not include eHealth services provided to citizens and patients (Sari et al., 2021).

Moreover, a study by Amankona et al. (2021) described that the necessary steps to generally mitigate security and privacy issues related to eHealth services are to implement appropriate policies, guidelines and regulations that adhere to applicable laws and follow the industry best practices standards. However, this study focused on the framework privacy by design to mitigate such issues and was thereby focused on the technical aspects of ensuring the security of eHealth services (Amankona et al., 2021). Therefore, this study is limited and does not take practitioners' experience into account in relation to ISMS or aspects such as human security behaviour.

3. Research Methodology

This chapter presents the methodologies for data gathering and analysis applied during the thesis project. Moreover, this chapter provides insight into how the research was designed and explains the thoughts and choices made throughout the thesis work. Firstly, the research approach is described. Secondly, the two applied methods for data gathering are presented: a systematic literature review and qualitative interviews. Thirdly, the methods for data analysis, thematic analysis, and qualitative content analysis (QCA), are described. This chapter ends with the presentation of ethical considerations and threats to validity.

3.1 Research Approach

The choice of research method depends on the aim and questions of the study because the knowledge that can be gained with each method differs (Eckerdal Rivano, 2016). To best address the research questions a qualitative research approach was chosen for this thesis work. This choice was validated by the description of qualitative methods given by Patton (2014) since they best fit research questions that are dynamic, complex and interdependent. Moreover, as explained by Almeida et al. (2017), unlike quantitative research, qualitative research is focused on aspects that cannot be quantified such as motives, values and attitudes.

Studies based on qualitative research are focused on the study of natural phenomena through the experience of people or communities, which also includes i.e., the context of the phenomena and the perspectives of which it is perceived (Busetto et al., 2020; Nguyen et al., 2022). Nguyen et al. (2022) also describe that qualitative research is supposed to be aimed towards the development of knowledge that has the power to make a difference thanks to the enhancement of intellectual evidence. The choice of qualitative research instead of quantitative research is supported by qualitative methods being especially suitable for studies of complex multicomponent interventions or systems (Busetto et al., 2020; Eckerdal Rivano, 2016). Moreover, by applying a qualitative research method such as interviews it allows for data collection from specific persons of interest from specific organisations (Recker, 2012).

Applying qualitative research methods require both time and resources since the method of choice must be planned, prepared, conducted, processed and analysed (Johnson & Onwuegbuzie, 2004). Also, to ensure the credibility of the collected data the methods must be presented through detailed descriptions, which also require time and attention. Another benefit of providing detailed descriptions of the data collection methods is that it assists in helping the data to be understood correctly (Schultze & Avital, 2011).

Although, a risk with conducting qualitative research is that the respondents' answers are up to the researcher's interpretation and can therefore be interpreted incorrectly, which is usually influenced by the researcher's values and beliefs (Johnson & Onwuegbuzie, 2004; Recker, 2012). Thus, research ethics has to be a priority so that the reader can be guaranteed that both the data collection and

analysis have been developed and conducted appropriately (Johnson & Onwuegbuzie, 2004; Recker, 2012). Concerning the work presented in this thesis, Schultze & Avital (2011) have argued that research within the area of Information Systems has been lacking proper descriptions of the utilised data collection methods, which is why every step of the data collection methods applied in this work are meticulously described in rich detail.

Moreover, through triangulation in research (e.g., the use of more than one research approach or method) the confidence and credibility of the findings increase (Heale & Forbes, 2013). In short, triangulation refers to the utilisation of multiple methods or data sources which is used to provide a more thorough understanding of the phenomena in question. This is also positive for the trustworthiness of the research because of the conjunction of information from different sources (Carter et al., 2014). Also, as stated by Heale & Forbes (2013) the combined findings of two rigorous research methods provide a more exhaustive representation of the results than either could do individually. Thus, the choice of applying two data collection methods is supported since collecting data from a combination of methods and sources assist in triangulating the findings (Arksey & Knight, 1999; Carter et al., 2014; Heale & Forbes, 2013).

Inspired by the description provided by Busetto et al. (2020) of qualitative research having the characteristics of flexible, responsive and an iterative process, a graphical process model for the research process of the thesis work has been visualised below (Figure 3).

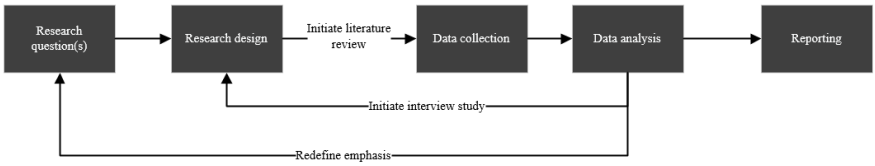

Figure 3. The research process of the thesis work

3.2 Systematic Literature Review

A systematic literature review is often applied to examine if previously evaluated data support existing or help in the creation of new hypotheses. Moreover, this method is commonly applied to support and present the background for upcoming research projects (Kitchenham, 2004). Rowe (2014) also emphasises that a well-conducted literature review can be applied to summarise, critically assist, explain results of and clarify prior research and therefore identify significant knowledge gaps. Considering that the work conducted during this thesis project included examining many previous studies, the characteristics of a systematic literature review supported the choice of that method as the primary data collection method.

The benefits of a systematic literature review are that the research is better equipped when evaluating the search in its entirety and with objectivity. Therefore, a systematic literature review in comparison to other reviews has the characteristics that allow for greater levels of objectivity. For that reason, a literature review was appropriate for the thesis work since it would allow for gaining better knowledge of the issues related to ISMS and privacy regarding the use of PeHS.

To achieve a high-level literature review one of the vital initial steps was to formulate a proper research question or aim of the review. By spending time on this step the rest of the review had a well-founded basis to rest upon and it set the stage for the rest of the review's structure (Jesson et al., 2011).

The purpose of the literature review in this thesis work was to examine what challenges have been found regarding ISMS and privacy when providing PeHS. Moreover, by conducting the literature review an interview guide for the qualitative interviews could be designed based on prior research. Therefore, the literature review was aimed to primarily provide answers to the first research question presented in chapter 1.3. As Jesson et al. (2011) describe, the review's aim/question is influential on later steps in the review such as defining search terms and publication selection criteria. Moreover, the review's aim/question also assists in setting the boundaries of the review as it helps determine which publications should be included in the review. For example, with this thesis work, publications dealing exclusively with the history of PeHS or testing different technical setups of the PeHS might not be of interest.

By conducting the review systematically, the reproducibility is greater, and the quality of the review is ensured (Rowe, 2014). To review and summarise the current state of research related to a particular phenomenon or topic, such as the challenges with ISMS and privacy regarding the use of PeHS, a systematic literature review can be utilised (Kitchenham, 2004). Moreover, according to Kitchenham (2004), the process of a literature review can simply be summarised into three phases: prepare the review, conducting the review, and reporting the review. These phases can be further explained with help by Jesson et al. (2011, p. 12) "*a review with a clearly stated purpose, a question, a defined search approach, stating inclusion and exclusion criteria, producing a qualitative appraisal of articles*". Moreover, the process of a literature review has been described as a combination of stages, which can be summarised as the following (Jesson et al., 2011; Okoli, 2015; Rowe, 2014):

1. **Define an appropriate research question** - Clearly define the purpose, goal, and research question for the review, as explicitly as possible.
2. **Design an execution plan** - Agree upon the procedure to follow and ensure that it is performed consistently by all involved reviewers.
3. **Search for literature** - Perform the search and describe how it was the reviewer ensured comprehensiveness during the screening process.
4. **Apply selection criteria** - Apply the predefined inclusion and exclusion criteria on the publications found during the literature search.
5. **Appraise the quality of publications** - Explicitly describe the criteria used to exclude studies based on insufficient quality.
6. **Synthesise the results** - Through analysis of the included studies combine information from the studies by appropriate methods.

A clearly defined search strategy is essential to ensure that the literature review is conducted systematically and correctly. Moreover, it is important to present the review strategy transparently and sufficiently to allow the reader to assess the strategy and if it has been completely and properly applied. By doing this the researcher can also avoid biased article selection and allow for greater replicabil-

ity (Kitchenham, 2004). It is also to the researcher's benefit to continuously document the review process to allow for a greater understanding of the progression of the review and increase the potential of implementing adjustments if necessary (Jesson et al., 2011). Moreover, Kitchenham (2004) describe that there are several documentation parameters that the researcher should clearly state in the research to achieve a high level of documentation and the following are the ones taken into consideration for the thesis work:

- Utilised database resources,
- Utilised search terms,
- Publication selection criteria,
- Date of each unique search, and
- Number of hits for each unique search.

Inspired by the framework presented by Meline (2006) the structure of the literature review was divided into three phases with several steps. The entire literature review process described in this subchapter has been visualised by a graphical process model presented in the format of a flow diagram presented below in Figure 4.

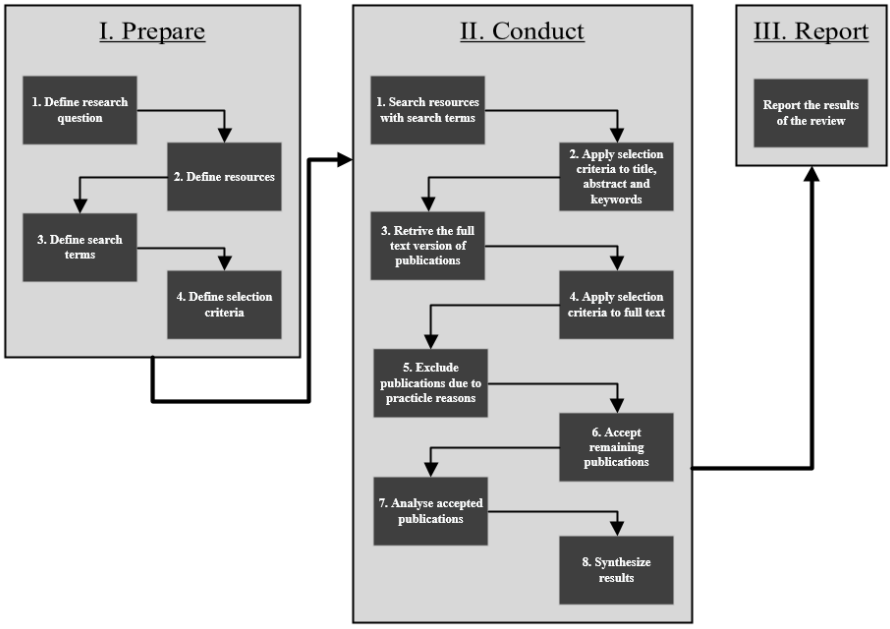

Figure 4. Flow diagram of the literature review process

3.2.1 Databases

In service of reproducibility and to make it possible for the reader to evaluate the applied method, the researcher should predefine in preparation of the review and disclose after the review which resources and search terms have been applied (Kitchenham, 2004). Moreover, Brereton et al. (2007) suggest that multiple database resources should be queried since no single resource is likely to find all relevant publications.

To ensure a greater likelihood of finding relevant publications for the review, four database resources were selected for the thesis work. Also, since some databases require the reader to pay for access to read the publications, free access is a fundamental requirement for the success of the literature review conducted in this thesis work. Because of this, only resources accessible through the University were considered and the University of Skövde allows for free entry to approximately 90 databases of varying fields of science. All the chosen database resources were recommended by DOME representatives, which were:

- PubMed,
- Medline (EBSCO), and
- Scopus.

3.2.2 Search Terms

One important task in the process of properly conducting a systematic literature review is to clearly define which search terms to apply during the selection phase. The search terms can affect the successfulness of the review if not carefully chosen because it influences the quality and completeness of the review as a whole (Jesson et al., 2011).

Therefore, topic-related keywords must be taken into consideration and that requires awareness of the topic. Otherwise, a reasonable bibliography of publications cannot be created and that is crucial for the review. Moreover, consideration must be taken to any synonyms or variations in spelling to increase the likelihood of finding all publications of interest. Although, the sheer number of search results and false-positive hits that need to be excluded can be overwhelming. Therefore, the researcher is recommended to match the work resources in terms of time, number of researchers etc. (Wohlin et al., 2012).

To improve the search process the researcher should also utilise Boolean operators (OR, AND etc.) (Jesson et al., 2011), which will also refine the search strings (Kitchenham, 2004). Although only a limited number of database search engines are designed to be utilised for systematic literature reviews. The databases simply treat search strings and Boolean operators differently. In addition, the results of the searches are also presented according to varying sorting. This means that the search term combinations must be adjusted according to the utilised databases (Brereton et al., 2007).

To maximise the publication search for this thesis work, the search terms and Boolean operators were defined in collaboration with DOME and the project available resources with deep insight into how the databases operate. Moreover, applicable synonyms, such as the ones for electronic health records, were applied to broaden the search inclusion. These synonyms were determined by looking up the term on the website Swedish Medical Subject Headings (MeSH) (Karolinska Institutet, n.d.). The following are examples of search terms used during the searches (the complete search terms can be found in Appendix A): Information security, Management system, ISMS, eHealth, PeHS, Privacy, and Data.

3.2.3 Publication Selection Criteria

According to Kitchenham (2004) and Wohlin et al. (2012) selection criteria should be used to assess the suitability of publications during the search process

in literature review. Inclusion and exclusion criteria are meant to identify primary studies that have a direct association with the research question while also excluding those studies that do not apply to the review. These criteria should be defined before initiating the search process to minimise the likelihood of bias. Furthermore, these criteria should be based on the research question and tested before the search to confirm that studies can be filtered. Although, it is important to acknowledge that the criteria are not static and might need adjustments as they are applied to the publications found through the resource searches. This could become relevant if the researcher finds that not all relevant aspects of the research were known before the search was initiated (Wohlin et al., 2012). The inclusion and exclusion criteria for the thesis work are listed below (Table 1).

Table 1. Applied selection criteria for articles

Inclusion Criteria	IC1: Published between 2012-2022
	IC2: Published in journal or conference
	IC3: Peer-reviewed
	IC4: Written in English or Swedish
	IC5: Publication is relevant to the research topic
Exclusion Criteria	EC1: Publication fails to meet inclusion criteria
	EC2: Publication occurs more than once
	EC3: Payment or additional login is required for access to the publication
	EC4: Inadequate description of results
	EC5: Exclude due to practical reasons (e.g., lack of applicable results)

The criterion IC1 defines the acceptable time frame of publication dates. Any publications from earlier years were therefore disregarded to limit the scope of the review. To ensure the quality of the publications included in the review criterion IC2 was defined, which stipulates that the publications must either be published in a journal or conference. To further ensure the quality of the review the publications must have been peer-reviewed. By setting that criterion (IC3) the publications considered for the review have already gone through an evaluation process to guarantee their quality (Loyd Sealy Library, 2018). To help determine if a publication has been peer-reviewed the global directory Ulrichsweb (*Ulrichsweb; Global Serials Directory*, n.d.) was utilised. Ulrichsweb contains detailed information (e.g., ISSN, publisher, language) about more than 300,000 serials of types such as e-journals, peer-reviewed titles, popular magazines etc. Access to Ulrichsweb is gained through the University of Skövde.

Moreover, since most studies within the field of information technologies are published in English that language is required for the thesis work and considering that the thesis project is conducted at a Swedish university, publications written in Swedish will also be included (IC4). The fifth inclusion criterion (IC5) helps determine whether the publications should be included even though they may have fulfilled the previous inclusion criteria since it considers the publications' relevance to the thesis work. In addition, the exclusion criteria further assist in assuring that publications are relevant for the thesis work and have the appropriate quality. Criterion EC4 specifically assists in determining if publications should be excluded even though there is a high relevance, but the description of the results is lacking. Lastly, publications could also be excluded due to not presenting any applicable results, which was determined at the very end of the selection process (EC5).

3.2.4 Backwards Snowballing

To allow for greater identification of applicable publications for the systematic literature review, the review was complemented with the data collection method backwards snowballing. The reasoning behind this is that the use of database searches alone is not a guarantee for finding relevant studies for the review (Kitchenham, 2004). Of course, this adds a heavy burden to the already demanding work of the systematic literature review. This would explain why the method of systematic literature review, unfortunately, fails to make use of additional methods such as backward snowballing. The extra effort simply is not worth it to some researchers (Wohlin, 2014). Although, the benefit of backward snowballing is that it limits the impact of the exclusion of potential publications done earlier in the literature review. This method is also beneficial to junior researchers and students that want to broaden their research by looking into findings from other research areas (van Haastrecht, 2021).

The method of snowballing for literature reviews has been described by (Jalali & Wohlin, 2012) as a method including three steps:

1) Use the accepted publications (from journals or conferences) as the input value and collect references from these publications,
2) Go backwards and collect references until no new references can be identified (repeat steps 1 and 2), and
3) Go forwards and collect publications that have cited the publications found in the backward snowballing.

Moreover, Wohlin (2014) emphasised that the publications used as the starting point of the backward snowballing must be valid to not negatively affect the snowballing procedure. Yet, he also explained that there is no right or simple way of determining the content value of the publications used as the input value.

Considering the description given by Jalali & Wohlin (2012) the following process has been performed. The references of the accepted publications from the database searches were collected and were thereby used as the starting set for the snowballing. These references were then evaluated according to the selection criteria presented in chapter 3.2.3. If the references pass all the inclusion criteria and do not fulfil any of the exclusion criteria, they are accepted into the review. The entire backward snowballing process described in this subchapter has been visualised by a graphical process model presented in the format of a flow diagram presented below in Figure 5

Due to the prerequisites of the thesis work, some limitations to the snowballing process were applied. Firstly, any publications found as references that had already been excluded during the database search selection process were automatically disregarded and not re-evaluated. Secondly, only one iteration of snowballing was applied. This simply means that only the references of the accepted publications were considered, not the references of any publication that pass the snowballing procedure. The reasons for this are the time and resource limitations of the thesis work.

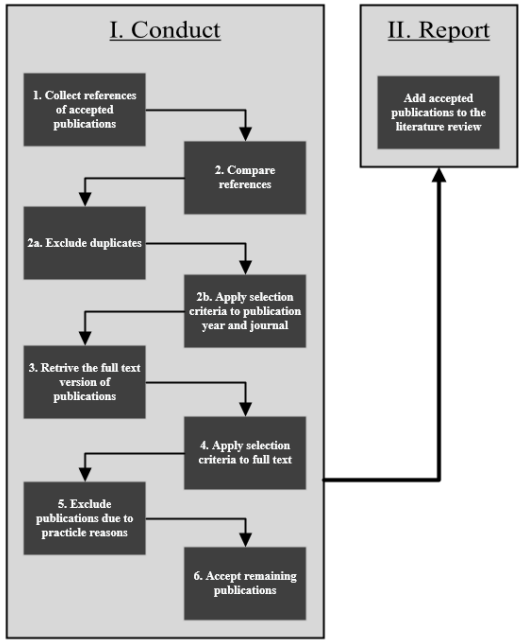

Figure 5. Flow diagram of the backward snowballing process

3.3 Qualitative Interviews

Arguably, the best way of gaining insight into how a group of people think about a specific topic is to ask them directly (Eckerdal Rivano, 2016; Schultze & Avital, 2011). This is also the data collection method applied by most qualitative researchers when the aim is to explore topics in-depth. The reasons for this are that interviews facilitate spontaneity, flexibility, and responsiveness from the respondents (Carter et al., 2014). Therefore, to gain insight into how practitioners are dealing with challenges related to PeHS concerning ISMS and privacy the second data collection method of this thesis was qualitative interviews. Interviews as a research method are used to obtain knowledge, experiences, opinions, and motivations from participants, not facts per se nor behaviours (Busetto et al., 2020; Schultze & Avital, 2011). This method is known as the most applied data collection method within qualitative research and there are several forms of interviews available to conduct (Eckerdal Rivano, 2016).

By conducting interviews, the researcher has the opportunity to discuss with the participant and gain deeper insight into their knowledge by questioning their thoughts, positions and experience (Alvehus, 2013). Some refer to interviews as dialogue (Huckvale et al., 2010), which could potentially be less taxing to potential participants in comparison to answering a lengthy survey. Because of the characteristic of being similar to a dialogue this method allows for a greater understanding and possibly more profound answers given by the participants (Alvehus, 2013), and in comparison to, i.e. surveys, qualitative interviews could result in unexpected topics being brought up by participants or the researcher based on the participants' answers (Busetto et al., 2020).

Although there are advantages to this method, there are also disadvantages to consider. For one, the interviewee could answer the researcher's questions as the researcher themselves wishes. Or the interviewee could simply answer poorly so not enough or nuanced data is collected (Recker, 2012). Criticism towards the method has also been brought forward due to the discussions on what knowledge the research might gain from conducting interviews. The question is if the context of the interviews might affect the outcome of the interview. Because of this, the researcher should acknowledge the context and how the interview questions are formulated (Eckerdal Rivano, 2016). Moreover, Almeida et al. (2017) emphasised that the use of interviews as the collection method is time-consuming since it requires considerable preparation for pre-interview and handling pre-analysis. Yet, this method of data collection has still been evaluated as the most fitting for gathering information from the participants since it allows for exploring areas within the research topic that the participants themselves reveal during the interviews.

The most common approach for interviews as data collection is semi-structured interviews (Recker, 2013). Semi-structured interviews can be described as interviews using open-ended questions and sub-questions, conducted according to an interview guide which defines general areas of interest. The questions and topics of the interview can be drawn from previous research or from the results of another data collection method (Busetto et al., 2020; Recker, 2012). There are several advantages to this type of interview application. For example, semi-structured interviews have been proven to be versatile and flexible, and they also allow for mutuality between the respondent and interviewer which enables a better quality of the follow-up questions (Kallio et al., 2016). By conducting semi-structured interviews there is room available for discussion or unique follow-up questions based on the participants' answers during the interview, so even with the predefined interview guide, there is more flexibility to this method (Alvehus, 2013; Recker, 2012).

As described by (Eckerdal Rivano, 2016) and (Kallio et al., 2016) the interview guide during semi-structured interviews should be divided into themes of interest to cover, but it should not define the sequence of the themes. All of this assists the interviewer to develop the interview as a conversation rather than an inquiry. Furthermore, as stated by Kallio et al. (2016, p. 2955) "*the semi-structured format is the most frequently used interview technique in qualitative research and in a healthcare context.*" However, the application of this type of interview requires that the interviewer has a certain level of knowledge of previous studies in the research area since the interview guide should be based on previous knowledge (Kallio et al., 2016). In this thesis work, a literature review was performed, and the results of the review were used to formulate the interview questions. Therefore, an understanding of the research area was gained, and it was possible to both design an appropriate interview guide and potentially coming up with follow-up questions on the spot depending on the respondents' answers during the interviews.

The unpredictability of Covid-19 has presented unique trials to the conduct of qualitative research (Pocock et al., 2021), the choice of interviews was still possible considering the technical possibilities and that interviews conducted face-to-face are not superior to other ways of interviewing (Sturges & Hanrahan,

2004). Pocock et al. (2021, p. 2403) stated "*there are many similarities between virtual qualitative research and traditional qualitative methods*".

Therefore, because of the chance of stricter public health measures, such as recommendations to work from home, the plan for the interviews was always to conduct them via virtual platforms (such as Microsoft Teams). The key point with virtual qualitative research is the use of virtual communication technology (Pocock et al., 2021) and because of this, the choice of virtual platform was based on the available virtual meeting platforms available to the participants. The plan was to conduct between three to six interviews over Zoom, where the participants would be a mix of regional representatives within Sweden. Moreover, the aim was to conduct the interviews between 40-60 minutes depending on how saturated the interviews were. To be able to perform an adequate analysis of the interviews the plan was also to record all the interviews, preferable with both audio and video to help facilitate the transcription of the interviews.

3.3.1 Sample Selection

The sample selection for this thesis work was determined through the selection already done by DOME. Moreover, the communication with the interview participants was done through representatives from DOME since that gave more weight to the participation requests. The discussions about the sample selection with DOME started before the beginning of the thesis work and carried on throughout the thesis work. The goal with the selection for the thesis work was to primarily interview participants with roles of Chief information security officer (CISO) or Data protection officer (DPO) within Sweden, either on a national or regional level.

The potential participants of this thesis work were required to have knowledge of the implemented ISMS for the PeHS available for the citizens or knowledge about any privacy concerns in relation to these services. Whether or not the region had experienced challenges that they also managed to mitigate was not deemed important since the focus of the interviews was to collect data to be able to answer the second research question. This meant that the identification of challenges and thoughts about them were more important than if the challenges were current at the time of the interview.

The reason for wanting participants with either the role of CISO or DPO was that they were determined to have the ultimate responsibility of the information security work and actions regarding privacy throughout the nation or region. Therefore, these participants were appropriate for interviewing regarding challenges with ISMS and privacy concerning PeHS. Below in Table 2, a short summary of the respondents is presented.

Table 2. Summary of Respondent details

Respondent	County	Position
R1	A	Function leader information security
R2	A	CISO
R3	B	Cybersecurity specialist

3.3.2 Design of Interview Guide

An interview guide was designed in preparation for the semi-structured interviews and the design was influenced by the results of the previously conducted systematic literature review in this thesis work.

Once complete, the interview guide was corroborated with a representative from DOME to ensure the relevance of the questions, both with the aim of the thesis project and DOME research project. Since the interview guide was based on the results of the literature review it was divided into sections according to the different challenges that had been identified. The sections and questions are briefly explained below (the full interview guide can be found in Appendix C):

- **Intro questions** - The purpose of these questions was to get the attention of the interviewee, inform them of the interview process and topic, and get consent relevant to the documentation and handling of the interview data (use of the name, recording, etc.).
- **Section related to the ISMS process**
    - Question 1
        - Follow-up question
            - Second follow-up
    - ...
- **Section related to responsibility**
    - Question 1
- ...
- **End questions** - The purpose of these questions is to round off the interview, make sure that every aspect has been touched upon sufficiently and allow for the interviewee to add before concluding the session.

3.4 Data Analysis Method

This subchapter presents the two methods of data analysis that have been applied during the thesis work. The first method, thematic analysis, was performed during the synthesising of the systematic literature review. The second method, qualitative content analysis, was performed in relation to the data collected during the semi-structured interviews.

3.4.1 Thematic Analysis

The synthesising of the review was performed by analysing the collected publications through thematic analysis, which according to Braun & Clarke (2006) is a flexible analysis method appropriate for qualitative research. Moreover, this analysis method has been described as a suitable introductory method to other forms of qualitative analysis since thematic analysis does not require that the research has detailed theoretical and technological knowledge of other qualitative approaches (Braun & Clarke, 2006).

This analysis method was deemed appropriate based on its applicability as stated by Nowell et al. (2017, p. 2) "*thematic analysis is also useful for summarising key features of a large data set, as it forces the researcher to take a well-structured approach to handling data, helping to produce a clear and organised final report*". However, there are known disadvantages to this analysis method that should be considered. For example, there is a lack of literature on the

method itself in comparison to other methods such as grounded theory, ethnography, and phenomenology, which could confuse researchers who lack the experience (Nowell et al., 2017). To mitigate this other research applying thematic analysis have been studied as reference studies in preparation for the synthesis of the systematic literature review.

The process of thematic analysis is done by identifying and evaluating patterns within the collected data. When the patterns have been identified, they are compared and enhanced until themes relevant to the research study can be defined (Braun & Clarke, 2006). As stated by Nowell et al. (2017, p. 2) "*a rigorous thematic analysis can produce trustworthy and insightful findings*". The thematic analysis for this thesis work was performed on a high level due to the time limitation. The thematic analysis process is presented below and it was inspired by the processes given by Nowell et al. (2017):

1 **Generate initial themes** - During the first readthrough of each publication codes were given to each publication, the codes functioned as the base for defining initial themes that guided the analysis based on similar codes.
2 **Search for themes** - When all the publications had been assigned codes the publications were grouped based on the codes and read through once more (or several times) during which themes were identified for the groups.
3 **Review themes** - During the third step all the themes were reviewed to determine if the groups shared similar or duplicate themes. This allowed for refining the themes and finding themes with a greater number of publications when applicable.
4 **Define and name themes** - Finally, once a list of themes had been collected each theme was defined, named, and described based on the connected publications.

3.4.2 Qualitative Content Analysis

As described by Busetto et al. (2020), the interviews conducted for the data collection have to be transcribed to allow for data analysis. Moreover, during the transcribing of the interview sessions, the researcher can decide to transcribe the interviews in their entirety including for example, filler words. The level at which the interviews are transcribed depends on what is relevant for the analysis. The planned method for data analysis is qualitative content analysis, which can be conducted on any type of material (notes, videotapes etc.) (Mayring, 2000) and the analysis with this method can be performed in various ways thus be suitable to researchers' of different levels of experience and knowledge (Lindgren et al., 2020). This method of data analysis can be described as a combined group of analytic approaches ranging from impressionistic, intuitive and interpretive analysis to systematic strict textual analysis (Prasad, 2019).

With this method for data analysis, the researcher must look for the different layers of content in the material, the primary content being topics and trains of thoughts while the latent content is developed through interpretation of the text (Mayring, 2000). Roller (2019) also explains that QCA can be described in different ways depending on perspective, two ways describing this method is that QCA is "*a systematic qualitative description of manifest content*" (p.1) and another that QCA is a method applied for a subjective understanding of "*patterns, themes and categories important to social reality*" (p.1). Therefore, QCA is an empirical, systematic approach-controlled evaluation of larger text masses, in

which the material is embedded in its communication context (Mayring, 2000). QCA is characterised as a method that is systematic, flexible and can reduce data, and therefore QCA is both data-driven and concept-driven (Prasad, 2019). In addition, by applying this method the research is focused on the subject and context while emphasising the differences and similarities between codes and categories (Graneheim & Lundman, 2004). With that said, this method is not about counting words or simply extracting content from texts, but the process of QCA includes analysing meanings, themes and patterns within the text (Prasad, 2019).

Graneheim & Lundman (2004) explain that the categories created during the data analysis of QCA can be described as the 'what?' and includes a collection of codes that can be sorted into the same group. Moreover, they explain that a theme should be considered an identified 'red threat' and a theme can include more than one category. Therefore, themes run through the data. In addition, Graneheim & Lundman (2004) explain that there is no 'correct' order of defining categories or themes, instead, they state that the richness of the data and the expressiveness of the codes are what determines what is defined first. Busetto et al. (2020) also declare that the process of coding is to relate raw data with theoretical terms and that allows for the data to be sortable.

For this thesis work the QCA was performed to produce a preliminary result of the qualitative interview, a further analysis will be conducted with the DOME research project in which the interview material collected during the thesis work will be included. However, the concepts of QCA have been reviewed and applied according to their relevance, so the qualitative content analysis has been performed in detail even though the analysis is preliminary.

Concepts

There are several concepts to acknowledge when conducting a QCA. The following are four concepts as described by Graneheim & Lundman (2004) relevant to the thesis work:

- **Meaning unit** - The combination of words or phrases that refer to the same meaning. Could be different words with common aspects and therefore relate to each other based on their content and context.
- **Code** - The label of a meaning unit, which allows for the material to be evaluated in new and different ways.
- **Category** - Refers to content that has been grouped according to their shared aspects. Could include subcategories that enhance the richness of the description of the material.
- **Theme** - A way of linking any underlying meanings in one category or across several categories. A theme can also incorporate subthemes.

3.5 Ethical Considerations

Ethical issues can reveal themselves during the research process from several perspectives such as the topic of the research, chosen methods and the presentation of the results. Therefore, consideration of ethical aspects was taken throughout the thesis work (Berndtsson et al., 2008; Recker, 2012; Roig, 2006). Regarding the thesis work, for the qualitative interviews the following ethical considerations were taken: informed consent, removal of audio- and videotaped recordings, confidentiality, and anonymity.

Moreover, each participant was informed in a clear and instructive way before the interviews that the material that was going to be collected during the interview would also be utilised in the larger research project conducted by DOME. At which point they could choose to not partake in the interview or elaborate on their consent regarding the handling of the audio and videotaped recordings from the interviews. Also, the interview participants were repeatedly informed about the purpose and aim of the thesis project. This was done both by the DOME representative who had the initial contact with the potential participants and then again when the participants were contacted with an invitation to the interview session, once by email and again during the introduction of each interview.

As part of the interview introduction the participants were informed that their names would not be declared in any collected or produced thesis work material. They were also asked to consent to the declaration of their organisational and regional affiliation in the material. In addition, as to the ethical consideration of confidentiality, the participants reviewed the transcribed material from their interviews and the whole thesis report before publication. Thereby, the participants themselves were able to retract answers if they for whatever reason deemed that it could lead to a breach of confidentiality of their person or their region. As for the research approach for the thesis project, the choice of methods was discussed with experienced and recognized researchers within the research area. Moreover, the research methods were based on well-established publications by recognized authors. Also, to maintain the context correctness, efforts were made to correctly citate the applied research in their appropriate context.

3.6 Threats to Validity

Ensuring the level of validity of the thesis work has been a high priority. As Wohlin et al. (2012, p. 68) stated "*the validity of a study denotes the trustworthiness of the results, and to what extent the results are true and not biased by the researcher's subjective point of view*". This is ensured by taking the following into account: internal validity, external validity, reliability and objectivity (Wohlin et al., 2012). Although, since this thesis work is a qualitative research study characterised as a naturalistic work the terminology presented by Shenton (2004) and Ngozwana (2018) will be applied, which in short can be explained as the following:

- 'Credibility' will be used instead of 'internal validity',
- 'Transferability' will be used instead of 'external validity',
- 'Dependability' will be used instead of 'reliability', and
- 'Confirmability' will be used instead of 'objectivity'.

These four qualities determine the trustworthiness of a qualitative research study (Shenton, 2004) and therefore, the term 'trustworthiness' will be applied throughout the thesis work instead of the term 'validity'. Considerable time was spent throughout the thesis project on identifying, assessing, and monitoring any potential threats to the trustworthiness of the thesis work. Especially the process for the systematic literature review which was conducted rapidly at the beginning of the project. Below the different strategies to ensure trustworthiness are explained further in individual subchapters.

3.6.1 Credibility

One of the most important aspects of the trustworthiness of qualitative research is to ensure that the study measures what it is supposed to measure a high level of credibility must be achieved. There are several vital aspects for the researcher to consider to ensure the credibility of their research (Shenton, 2004). Hence, the following five applicable aspects have been taken into consideration for the thesis work:

- **Choice of research method** - The chosen method should be well established in both general qualitative research and information science. Should be developed, if possible, from previously comparable research projects where the method has been successfully applied.
- **Triangulation** - By applying different research methods the methods could compensate for their individual limitations and therefore strengthen the research.
- **Debriefing** - To increase the credibility of the research continuous debriefing session should take place between the researcher and the supervisor. This allows for improvements of the study based on the supervisor's experience and perceptions. Moreover, such sessions could be utilised to test and develop ideas, interpretations, and assist in identifying biases or preferences.
- **Peer-review** - If available, opportunities for feedback from peers or academics during the research study should be welcomed since it will allow for another's perspective. This could help the researcher to e.g., refine methods, mitigate a lack of proper descriptions, and strengthen the motivations of the study.
- **Examining previous research** – It is essential to the credibility of the study to examine the study's results and assess the congruence with previous research. A key aspect is therefore to relate the study's findings to the existing body of knowledge in the research area.

Initially, a threat to the trustworthiness of the thesis work was identified as related to the unfamiliarity of the research area. To mitigate this a broader research aim was defined in preparation for the systematic literature review and then redefined while the thesis work progressed. By doing this the aim of the thesis work got more focused and detailed since more knowledge in the research area had been gathered. Moreover, check-ins regarding critical points during the thesis work (e.g., choice of research method, use of search terms, design of selection criteria) have been made with experienced researchers from the DOME project and the thesis project supervisor to ensure the quality and trustworthiness of the thesis work. Also, before publishing, the thesis work was peer-reviewed by two other master students. All of this helped improve the credibility of the thesis work.

In addition, to further ensure the credibility of the thesis work, previous research was elaborately examined, both within the systematic literature review and as part of presenting related works within the research area. Moreover, the choice of research methods was discussed several times with experienced researchers within the research area and evaluated throughout the process of the thesis work to ensure that the appropriate method was chosen and correctly applied.

3.6.2 Transferability

Due to the nature of the findings of qualitative projects being specific to a limited number of environments and individuals, it is difficult to demonstrate transferability to other situations or populations. To deal with this the researcher should provide a description of the contextual factors impacting the research, which could include the participating organisations, restrictions during the data collection, applied data collection methods and information regarding the data collection sessions (Shenton, 2004). To ensure the transferability and dependability of the thesis work all research methods applied and choices made during the thesis project have been transparently explained in detail. Moreover, the delimitations of the thesis work (see chapter 1.4) have been clearly defined before any data collection has begun.

3.6.3 Dependability

To deal with the issue of dependability of a study the research should transparently and in detail report on the study's process. By doing this a future researcher could utilise the study as a prototype model for their own research. In addition, by reporting on the study's process in this way the reader can assess the level at which the researcher has followed proper research practices. This type of report should include aspects from both the strategic and operational levels, such as the research design, implementation, data gathering and evaluation (Shenton, 2004). In addition, two different collection methods were applied to ensure triangulation and therefore improve both the credibility and the confirmability of the thesis work. Efforts have also been made to ensure the trustworthiness of the thesis by meticulously and transparently describing every step of the research process, choices made and any applied resources. This relates both to increasing the confirmability and dealing with the dependability of the thesis work.

3.6.4 Confirmability

A high level of confirmability of a study is achieved by ensuring that the findings of the work are the result of the informants and not the characteristics or the preferences of the researcher conducting the study. This can be assisted by the utilisation of triangulation since it reduces the effect of the researcher's potential bias. Moreover, it is essential that the work presents an 'audit trail' which allows for any reader to follow the study's process step-by-step, including detailed descriptions of all procedures and all decisions made (Shenton, 2004). Another potential threat to the trustworthiness of the thesis work was the issue of a lack of relevant publications found during the systematic literature review. To mitigate this a combination of database resources were utilised and the method of backwards snowballing was also applied. With these measures, the total number of publications from the database searches was drastically increased and through the backwards snowballing process several more publications were reviewed that initially did not show up during the database searches. These mitigations both increased the credibility and the confirmability of the thesis work.

4. Practical Application

In this chapter the practical application procedures of the data collection and data analysis methods are described to provide insight into the process and outcome. Firstly, the procedure regarding the systematic literature review is presented, which include information about the database search and backward snowballing results. Secondly, the procedure of the qualitative interviews is presented. Thirdly, the analysis procedure for both the literature review and interviews are presented in separate subchapters.

4.1 Practical Publication Selection Procedure

Figure 3, presented in chapter 3.2, illustrated the different phases and individual steps of the systematic literature review conducted during this thesis project. The first phase (Prepare) was further explained in chapters 3.2.1-3.2.3, which included a detailed description of the defined database resources, search terms and publication selection criteria. All of which made up the selection process's structure of the review. Moreover, the process of backward snowballing presented in chapter 3.2.4 and illustrated in Figure 4 also conveyed the different steps that were going to be taken during the review to gather further publications based on the references of those publications accepted during the selection process.

Below in chapter 4.1.1 the practical application of the selection process is presented which is equivalent to phase II (Conduct), steps 1-6. This includes reports on how the database resources were probed with the defined search terms and how the selection criteria were applied. This is followed by the practical application of the first phase of the backward snowballing process. Finally, the bibliography of the accepted publications is presented. These publications were upon acceptance moved to the analysis which is presented in chapter 4.3.1. The evaluation of the findings of the literature review is however presented in the results chapter (chapter 5).

4.1.1 Database Search

As presented in chapter 3.2.1, three database resources were probed with the search terms documented in Appendix A. In total, 18 search operations were conducted. The three database resources are independent entities with differences in user interfaces and available functionalities which in turn affect the searches. For example, the database resources offer different levels of filtering and therefore was the search terms applied on different levels, which is described below in Table 4.

Table 3. Utilized databases and which search terms were applied

Database	Search terms applied onto
PubMed	Publication year, publication type, text availability
Medline (EBSCO)	Publication year, publication type, text availability, text availability
Scopus	Title, abstract, keywords, publication year, publication type, publication source

Step 1 - Search resources with search terms

All the publications found during the searches were documented in one Excel-file. The parameters saved for each publication (if available) was applied search

term, resources database, authors, title, publication year and Doi. These parameters were found by downloading the search results from the databases in separate CSV files and by manipulating the files (separating the text into columns). The CVS files were manipulated, but this was not an easy task, resulting in much time spent trying to filter out the important information. Many of the parameters could be drawn from the files, but for some publications, the publication year and Doi could not be retrieved. This did not end up being a problem since the most important parameters were the publication title and authors' names. The searches resulted in 18,667 hits.

Step 2 - Apply selection criteria to the title, abstract and keywords

The first selection filtering was done through the removal of duplicates, which met the exclusion criteria EC2. This was accomplished by filtering the complete list of found publications in alphabetic order based on the column for titles and then based on sorting in the column for Doi. Each row was reviewed, and all duplicates were marked in a separate column (called IC/EC) with the code EC2. The first instance of the publication from the earliest database search was kept unmarked. Out of the initial 18,638 hits, 7,679 were found to be duplicates. The remaining number of publications was 10,988.

The searches were broad and therefore the second selection filtering was done by reviewing the titles of the publications to determine the publications' relevance to the research topic. This meant both looking into the publication's topic, but also characteristics such as the type of publication. This was done in accordance with step 2 of phase II presented in Figure 3. This made it possible to evaluate if the publications fulfilled the inclusion criteria IC2 (published in a journal or conference), IC3 (written in English or Swedish), IC4 (peer-reviewed) and IC5 (relevance to research topic). It is important to note that IC5 at this stage was determined on a first and superficial evaluation level. This criterion was evaluated again at a later stage. At this point, the title merely provided the first impression of a publication's topic and nature. Again, each row (that had not been marked EC2) was reviewed and either marked as 'EC1' or 'I?'.

This process allowed for discovering missed duplicates that were marked as EC2. By marketing each individual row, it was possible to determine at the end of the filtering that all rows had been reviewed and evaluated. The second filtering resulted in 10,824 publications being excluded, which resulted in 164 publications remaining (marked with 'I?'). Out of these 164 publications, some were more unclear than others because of the ambiguous or incomplete titles. Therefore, it was expected that several of them would probably be found as not applicable for the literature review once the full version of the publications had been reviewed.

Step 3 - Retrieve the full-text versions of publications

Upon trying to retrieve the full-text versions of the publications the abstracts were read, which allowed for several more publications to be excluded most of which due to their lack of relevance to the thesis' topic. At this step, 32 were disqualified due to criteria EC3 since they require payment or further log in to access the full publication. Which left 32 that could be retrieved in their full-text versions.

Step 4 - Apply selection criteria to full text

The next step was to apply all the selection criteria to the full-text version of the publications. To ensure that the publications met inclusion criteria IC3 (peer-reviewed) the global directory Ulrichsweb. Firstly, the publications were grouped according to their journal and then each of those journals was searched on Ulrichsweb. The conference papers were evaluated by visiting the conferences' own websites and checking if they have made a declaration of the included papers in their conferences being peer-reviewed. This process turned out to be rather strenuous since it took considerable time to find the required information. In the end, 10 publications were disqualified.

Next, the publications were evaluated based on selection criteria IC5 (relevance) and EC4 (quality), which were done firstly by searching for specific words relevant to the thesis work such as security, health, privacy, ISMS and more. When these words could not be found or their significance in the publication was not deemed enough the publication was excluded. Next, the articles that did include the words and were not excluded were read through in their entirety. In the end, another 9 publications were excluded of which 3 due to EC4.

Step 5 - Exclude publications due to practical reasons

The last step of the selection process was to exclude those publications due to practical reasons, which ended up being 9 publications. For most of those publications, the reason for exclusion was since their result did not add anything (positive nor negative) to the thesis work. Therefore, they held no value to the thesis work.

Step 6 - Accept remaining publications

After the selection process a total of 17 publications were accepted to the next step of the systematic literature review. Below an overview of the results from the literature search are presented, which indicates how many publications have been excluded and included in the review (Table 4).

Table 4. Literature review search overview

Database	Search date	Search term	Hits	EC1	EC2	EC3	EC4	EC5	Included
PubMed	2022-02-25	ST1	3	3	0	0	0	0	0
	2022-02-25	ST2	2	1	1	0	0	0	0
	2022-02-25	ST3	2	0	2	0	0	0	0
	2022-02-25	ST4	3,569	3,088	447	14	1	9	10
	2022-02-25	ST5	1,716	9	1,707	0	0	0	0
	2022-02-25	ST6	4,289	2,663	1,625	0	0	0	1
Medline	2022-03-05	ST1	9	8	1	0	0	0	0
	2022-03-07	ST2	3	1	2	0	0	0	0
	2022-03-07	ST3	9	7	2	0	0	0	0
	2022-03-08	ST4	181	12	169	0	0	0	0
	2022-03-08	ST5	88	1	87	0	0	0	0
	2022-03-08	ST6	3,347	3,034	310	3	0	0	0
Scopus	2022-03-05	ST1	270	262	5	1	0	0	1
	2022-03-05	ST2	8	3	5	0	0	0	0
	2022-03-05	ST3	35	20	13	2	0	0	0
	2022-03-05	ST4	1,821	1,271	535	8	1	0	5
	2022-03-07	ST5	1,796	121	1,672	2	1	0	0
	2022-03-07	ST6	1,519	420	1,096	2	0	0	0
Total			18,667	10,924	7,679	32	3	9	17

4.1.2 Backward Snowballing

As described previously, to increase the likelihood of identifying as many relevant publications as possible for the literature review backward snowballing was applied. The references of the 17 accepted publications from the database searches were all collected and documented in an Excel sheet. Again, parameters such as title, author's name, publication year and Doi were documented. These references were the input for the backward snowballing as described in Figure 4 (see chapter 3.2.4). The snowballing process was initiated 2022-03-21 and finished 2022-03-22.

Step 1 - Collect references of accepted publications

Each accepted publication's references were extracted by copying and pasting them into the Excel sheet without consideration regarding e.g., publication year or publication type. This resulted in a total of 1,060 rows.

Step 2a - Exclude duplicates

Similarly, to step 2 the first action once the references had been collected and organised was to exclude duplicates. This was done by comparing the list of references by title and authors and each reference was reviewed row by row through the Excel sheet. By doing this, 146 duplicates were removed, which meant that 914 remained.

Step 2b - Apply selection criteria to publication year and journal

The selection criteria concerning the publication year and publication type were then applied to the remaining references. During this step, 599 were removed due to not fulfilling inclusion criteria IC1 (allowed publication interval) and 58 for not fulfilling IC2 (allowed publication type). In the end, a total of 258 references remained.

Step 3 - Retrieve the full-text version of publications

The third step of the snowballing process was to retrieve the full-text version of the remaining references. This also made it possible to exclude 11 due to access availability (EC3) and another 19 items due to lack of connection to the thesis work based on the title or abstract (IC5). Upon retrieving the full-text version the language of the publications was also checked (IC4). The number of references with full-text versions ended up being 6.

Step 4 - Apply selection criteria to full text

Next, the remaining selection criteria IC3 (peer-reviewed), IC4 (language), IC5 (relevance) and EC4 (quality) were applied to the full-text versions. This was carried out in the same fashion as desired for step 4 of the selection process (chapter 4.1.1). No items were excluded during this step.

Step 5 - Exclude publications due to practical reasons

Lastly, 3 were excluded due to practical reasons such as lack of usable results which therefore meant that they would not add anything to the thesis work.

Step 6 - Accept remaining publications

Two items out of the 1,060 references pasted the selection criteria during the backwards snowballing process described in chapter 3.4.2. However, one of these items had already been accepted through the selection process and was therefore removed as a duplicate. Once the item from the backwards snowballing process had been added to the list of accepted publications the search process was concluded. Below an overview of the results from the backwards snowballing process is presented, which indicates how many publications have been excluded and included (Table 5).

Table 5. Backwards snowballing overview

Criteria	EC1	EC2	EC3	EC4	EC5	Included
	898	147	11	0	3	1
Total	1,059					

4.1.3 Final Bibliography

The selection process, including both database searches and backwards snowballing, has resulted in a final bibliography of 18 accepted publications that have been found relevant to the thesis work. All these publications have met the previously defined and explained inclusion criteria without fulfilling any of the exclusion criteria. Appendix B contains the complete collection of accepted publications. The bibliography has been presented in the form of a table in which each individual publication has been assigned an id (e.g., P01, P02 etc.). The ids were assigned in consecutive numbering according to the order in which the publications were accepted into the bibliography. By assigning a short id to the publications there is no need to refer to the full-scale reference construct when referencing any of the accepted publications, which assists in making the analysis text more fluent.

4.2 Practical Interview Procedure

Because of the size of the systematic literature review a decision was made that a limited number of interviews and respondents would be necessary to collaborate the results from the systematic literature review. This decision was discussed both with the thesis project supervisor and the representative from DOME. Considering this decision, two extensive interviews both in length and information were conducted with a total of three participants, and it was found that those interviewed were enough for the second data collection for this thesis work.

As described in chapter 3.3.1 (Sample Selection) the initial contact with potential participants was done through a representative from DOME. Date suggestions were discussed with the DOME representative before contact was made with potential participants. Once a person had agreed to participate their contact information was provided from DOME. From that point, the contact with the participant was managed as part of the thesis work. Starting with sending out an email with a meeting link to the agreed-upon date and time, and a brief explanation of the aim of the study. This was followed up by a second email one or two days before the planned interview and through that, the participants were provided with the interview questions. All communication was done in Swedish, both pre-interviews, during the interviews and post-interviews.

During the interview, the interview guide was followed (Appendix C) and that started with asking about consent from the participants, both for recording the interview and to use their organisational affiliation in the thesis work. All participants agreed to the recording of their interviews with the condition that the recording was only managed by the interviewer and deleted immediately once the material had been transcribed. Moreover, none of the participants consented to the use of their organisational affiliation in the thesis work and therefore only the participants' roles are provided in the thesis work. Each interview, which was conducted digitally, was held with video cameras turned on to allow for some face-to-face interaction. Also, a PowerPoint presentation was shared and utilised during the interviews to assist the participants in their understanding of the questions asked. The PowerPoint was designed based on the interviews guide and helped guide the interview conversations since the participants could follow along on their screens as the interview was ongoing.

Because of the sensitivity of the discussed topics in the interviews the participants were offered the chance to review the transcript material from their interviews and the thesis work, which also ensured the trustworthiness of the thesis work. The interviews were transcribed and sent to the corresponding participant for their approval before the material was used in the thesis work. Moreover, because of a lack of knowledge of some of the topics discussed during the interviews a participant from the first interview wished to investigate further within their organisation before providing answers to some of the questions. This was only seen as something positive since it would add more established data to the study, so the participant sent answers to a few questions a couple of days after the interview over email (Appendix F). Below in Table 6, a summary of the interviews is presented.

Table 6. Summary of Interview details

Respondent	Interview date	Communication channel	Duration	Appendix
R01	2022-04-26	Zoom	59 minutes	Appendix E
R02				
R03	2022-04-28	Zoom	43 minutes	Appendix G

4.3 Practical Analysis Procedure

In this subchapter the individual practical analysis procedures for thematic analysis and qualitative content analysis are presented. Each procedure is presented in rich detail according to the process descriptions given in chapter 3.4.

4.3.1 Analysis of Literature Review

The analysis process started with repeated read-throughs of each accepted publication during which codes were assigned to the individual publications based on their emphasis. During the read-throughs patterns regarding challenges with information security and privacy concerns were identified.

Once each publication had been assigned codes and no new codes could be found, the publications were grouped based on the codes. Then, the groups were reviewed, and each publication was read-through again to define themes. Once themes for each group had been identified, the themes were reviewed to check if groups shared similar themes that could be combined. Lastly, when a list of

themes for all the publications had been identified the themes were named. A total of 57 codes and 13 themes were defined, which are presented in Table 7.

Table 7. Overview of themes and related studies

Codes			Themes
Access control	Access monitoring	Access requirements	Should vs. Must have access
Wide access)	Inapplicable data use	Purpose based permission	
Emergency access	Balance (privacy vs. benefit		
Access trust	Control based on preferences	Privilege abuse	Trust vs. Control
Standards	Policies	GDPR compliance	Regulatory compliance
Human behaviour	Consent	Interchanging staff	The users
User safety caution			
IoT	Mobile devices	External applications	Applications
Attack surface	Cyberthreats	Employee misuse	Threats
Hacking threats	Insecure interfaces/APIs	Network threats	
Offline sharing	The value of medical data	Flawed IT infrastructure	
Secondary use	Potential of medical accidents		
Cultural view	Information security culture	Security culture	Culture
Data storage	Data management		Data lifecycle management
Cybersecurity	Information practices	Lack of knowledge	Knowledge
ISM awareness	Lack of research		
Cloud	Evidence based	Lacking encryption	The technology/design
End-user involvement in design			
Appropriate data	CIA	User anonymity	Data characteristics
Data volume	Data secrecy		
Multiple parties	Ownership	Interoperability	Interconnectivity
Accountability	Lack of auditing		Security practises

These themes should be viewed as challenges with ISMS and privacy related to PeHS. The correlation between the challenges and publications is illustrated in the matrix below (Figure 6).

Challenges / Publications	Total challenges per source	Should vs. Must have access	Trust vs. Control	Regulatory compliance	The users	Applications	Threats	Culture	Data lifecycle management	Knowledge	The technology/design	Data characteristics	Interconnectivity	Security practises
Total sources per challenge		8	7	5	6	5	11	3	5	9	6	3	11	3
P01 - Ishaq et al. (2021)	7	X	X		X		X				X	X		X
P02 - Oh et al. (2021)	4					X	X			X			X	
P03 - Priya et al. (2017)	2						X						X	
P04 - Özkar & Sandikkaya (2020)	4		X			X	X						X	
P05 - Cellier & Ghernaouti (2019)	6	X	X	X	X			X		X				
P06 - Kamoona & Altamimi (2018)	4	X									X	X	X	
P07 - Fragidis & Chatzoglou (2017)	1												X	
P08 - Lustgarten et al. (2020)	5				X				X	X	X	X		
P09 - Al-Issa et al. (2019)	4			X			X				X		X	
P10 - Kuo (2018)	4			X	X			X		X				
P11 - Ronquillo et al. (2018)	2						X						X	
P12 - Nurgalieva et al. (2020)	5		X				X			X	X		X	
P13 - Els & Cilliers (2017)	5		X	X		X	X		X					
P14 - Zegers et al. (2021)	7	X	X		X			X		X	X		X	
P15 - Sahi et al. (2018)	8	X	X	X		X	X		X	X				X
P16 - Edemacu et al. (2019)	4	X					X		X				X	
P17 - Bani Issa et al. (2020)	6	X			X				X	X			X	X
P18 - Coppolino et al. (2017)	4	X				X	X			X				

Figure 6. Matrix over challenges related studies

4.3.2 Analysis of Qualitative Interviews

The analysis process for the qualitative interviews started with the repeated read-throughs of the transcribed material and comparison between the material from the two interviews. During the read-throughs, codes were assigned to the respondents' answers, the aim of these codes was to help determine challenges with information security and privacy, and how challenges within these areas had been mitigated. The read-throughs concluded once no new codes could be found or assigned to any further answers, after which the answers were grouped based on the codes.

Then, the code groups were reviewed to determine appropriate examples of meaning units and define common categories for the different codes. Once the categories had been defined, reviewed to find, and combine similar categories, the final categories were reviewed again to define themes. A total of seven codes, three categories and two themes were found during the QCA analysis. Below the codes, meaning units, categories and themes are presented in more detail.

Meaning units

In Table 8 four examples of the meaning units found by analysing the collected material are presented, as well as the corresponding condensed meaning units and codes. The codes are further explained in the next subchapter.

Table 8. Meaning units from QCA

Meaning unit	Condensed meaning unit	Code ID
"All the structures and standardizations we have facilitate the dialogue we have with others."	Standardisation assists the dialogue	C02
"The more users, the more consumers of information, the more information we have and the more surfaces we have, the more vulnerable we are and then we need to work even more actively and efficiently based on the management system we have."	Digitalisation has made us more vulnerable and demands more efficient work processes	C04
"So, it is a challenge to catch up with the development that is taking place. Especially when we talk about connected to patient-centred services and the type of digitization that a patient-centred care requires and that the patient is in focus, and so on."	Difficult to keep up with the development of PeHS	C04
"One challenge is to try to have a sensible discussion about whether the service actually provides the patient with any real benefit. Usually it does, but sometimes there are some a little too crazy ideas that you have to resist."	Question ideas to allow for reasonable services	C07
"[...] the knowledge that it is also possible to provide access to information in medical records when young people are 13-15 years old needs to be clearer [...] If we are to increase the use of our PeHS, we get started better information about opportunities."	Increased use of PeHS requires better information to the end users	C01

Codes

The coding performed in the QCA for the material collected during the qualitative interviews was based on the analysis of the meaning units. Moreover, to efficiently code the interview material, a coding scheme was designed, which is presented below in Table 9.

Table 9. Codes from QCA

ID	Code	Description
C01	Opportunities for improvement	Relates to what the respondent has expressed has room for improvement which would improve the overall process for ISMS/privacy
C02	Assistance	Relates to what the respondents have identified as potential points of assistance to the design or implementation of the ISMS.
C03	Fend for yourself	Relates to that the respondents explained that each region or organisation is left to deal with ISMS and privacy issues on their own since it is ultimately their own region/organisation that owns the risks related to ISMS/privacy.
C04	Complexity	Relates to the issues or challenges related to the complexity of the situation in which the ISMS is supposed to be implemented.
C05	Progress or not	Relates to the progress that has or has not been made within ISMS or privacy. Such as how the implementation of GDPR has affected the progress of privacy within the organisation/region.
C06	Work process	Relates to several aspects of work processes, such as the overall ISMS process or process for implementation of PeHS. Including the process of assigning privileges or access rights to systems.
C07	Greater understanding	Relates to the lack of or improved understanding of ISMS and of how it should be implemented by the employees, patients, and citizens within the region.

Categories

From analysing the collected data from the qualitative interviews and comparing the identified codes with each other three categories were defined. These categories are explained below:

- **Sound prerequisites**
  The first category relates to the progress or lack of progress made within ISMS or privacy and if there is a lack of or improved understanding of ISMS among employees, patients, and citizens. What this comes down to is if there are sound prerequisites for an ISMS and privacy management within the organisation
- **The processes**
  The second category relates to the processes involved with ISMS and dealing with privacy concerns. Which includes what is and may assist in the design or implementation of the ISMS, but also what the respondents have described as difficulties with ISMS and privacy in relation to PeHS that makes the situation complex to handle. For example, the pace of digitalisation and the need to keep up with that in the ISMS process is challenging. Another example is that the development of legislation does not keep up with the pace of digitalisation and therefore new legislations are presented once the regions have already done work in the ISMS process and must backtrack and redo the work according to the new legislation.
- **Possible collaborations**
  The third and last category relates to what the respondent has described as room for improvement, which includes aspects such as improved communication within the region regarding PeHS to both healthcare personnel and citizens, and improved legislation which does not contradict each other or makes the ISMS process heavy. This category also relates to the fact that the regions are working alone and do not collaborate as much as they possibly could or would like to, which for example is because the regions themselves are owners of their risks.

Themes

The primary theme that emerged during the interview sessions and when analysing the collected interview material was the theme of knowledge. There are several aspects related to this theme. Firstly, understanding what ISMS entails and how to manage privacy concerns. Secondly, there is the challenge of dealing with the different ideas that healthcare personnel would like to implement and getting them to understand that the service must have a realistic and real benefit to the patient. Thirdly, although healthcare personnel might have embraced the use of PeHS and gotten better at communicating information to patients through the PeHS, they must also understand that a change in user behaviour (e.g., purposely entering data in an incorrect field in the EHR system) has consequences. This theme is anchored in the related works presented in chapter 2.2. Mense et al. (2013) explained that organisations unfortunately are likely to misunderstand the concept of information security, especially as something that mainly requires technical security controls. As with this theme, the misunderstanding of the concept could adhere to a lack of knowledge on ISMS and information security as an area.

The secondary theme relates to standardisation. This theme relates to the expressed benefits and strengths of standardisation, both within the own organisation and in collaboration or dialogue with other regions. Moreover, the respondents discussed the different aspects from which standardisation could emerge. On a national scale that could be national directions, support, and guidelines regarding the legislation that those who work with ISMS and privacy must take into consideration. It could also emerge from the use of standards such as the ISO 27000-series throughout the regions which would enable everyone to use the same language and terminology. Thereby enabling an easier dialogue between regions in this area. The perspective regarding legislation relates to the related work by Scandurra et al. (2017) that was presented in a previous chapter (see chapter 2.2) in which the researchers described that there is a gap between the legislation and the development of PAEHR. Moreover, as Scandurra et al. (2017) described, this gap could be the result of healthcare being a complex organisation with a necessary collaboration between several different actors.

In Table 10 below the relationship between the concepts defined for this thesis work is presented.

Table 10. Relationship between themes, categories, and codes from QCA

Themes	Knowledge	Standardisation	
Categories	Sound prerequisites	The processes	Collaboration
Codes	- Progress or not - Greater understanding	- Assistance - Work process - Complexity	- Opportunities for improvement - Fend for yourself

5. Results

In this fifth chapter, the results of the thesis work are presented. The results are both presented individually for each data collection method and jointly at the end of the chapter. The results are presented according to either the themes or categories identified during the analysis process described in chapter 4.3.

5.1 Results of the Literature Review

The results of the systematic literature review are presented below according to the 13 themes of challenges to ISMS and privacy related to PeHS that were identified during the data analysis.

5.1.1 Should vs. Must have access

The first challenge described by several researchers is the one related to access. Since PeHS include sensitive information about patients and people's medical history the question is whether a user should have versus must have access or not. Therefore, there are two contradictory requirements for access to patient data. On one hand, the data must be accessible by a large group of individuals simultaneously anywhere at any time and quickly to ensure efficient care. However, the data must also be sufficiently protected since a lack thereof could negatively affect the person's privacy (P05, P06). There is no straightforward answer for how to manage privacy with eHealth and therefore a balance must be achieved between individual privacy and potential benefit for each eHealth service. Researchers have found that individuals of e.g., ailing health are willing to trade-off some privacy for the benefit of better care and gain independence. However, most healthy adults insist on greater security and privacy for their PeHS (P14). In addition, the structure of the involved systems and classification of data within healthcare makes the challenge of access even more complicated, which is why some are likely to simply provide wider access than trying to limit access to certain groups (P05).

There is a multitude of perspectives to take into consideration concerning access. For one, there is the question of how to set up and manage the access control to manage the data access and data flow within the environment (P15). The fact is that without a proper access control mechanism users could cross intended boundaries and access more data than they should be able to access, both intentionally and accidentally (P16, P17, P18). This could be done by a user access policy based on the consequences user access poses when accessing the data (P01) or a role-based policy that declares the level of access based on the user's role (P06). Although, access control is not enough. Even with controls in place to limit data access, there is still going to require many users having access to patient records. Hence, PeHS providers should apply access monitoring. This too is complicated due to the large number of people having access to the services (P05).

Then there is the issue of the need for emergency data use. Due to the requirement of medical staff having to provide rapid care they must have access to patients' data quickly and without needing to specify what data they need in every unique situation. Yet again, the solution here has historically been to assign wider access which in turn has other consequences such as people processing

information without proper cause (P05). However, when looking at this perspective of the challenge of access one must take into consideration that access control in emergencies is more complex and difficult to approach. Thus, any access control also requires the possibility of bypassing any security access mechanisms in emergencies (P15). Lastly, concerning access, one must consider the possibility of someone without expert knowledge accessing and modifying patient data. This could in a worst-case scenario lead to improper diagnosis and faulty treatment of the patient. Moreover, with PeHS there are often multiple parties involved (such as system suppliers and different healthcare providers). The challenge is to assign and manage access based on positions, which could limit the possibility of unauthorized access or wrongful data management (P01).

5.1.2 Trust vs. Control

The second challenge also relates to access, but from the perspective of trusting the caregivers' data management versus the patient's control over their data (P05). Due to some eHealthcare providers' failure to preserve the privacy and security of patient data patient trust in their caregivers' management of patient data has decreased (P15). Moreover, the users (patients, nurses, physicians etc.) also must trust the technological solution (P04). Otherwise, they might change their behaviour and by doing so they might not use the systems correctly or not provide enough and proper information (P12). Some researchers take the standpoint that each individual person must own the power of access over their data (P01). Although, the challenge is made more complex when simply assigning patients control over their own data. Because doing so requires the patients to understand what that control entails and their options for sharing their data (P13, P14).

5.1.3 Regulatory compliance

Several researchers also describe the challenge and need to comply with standards and laws concerning eHealth (P15). Firstly, there is the ISO 27000-series which addresses information security and the concerns to take into consideration. This series is highly relatable since it also describes the best practices for information security management (ISM) within an ISMS (P09). Since information security and privacy concerns have been found to be the primary challenges PeHS providers must design a sufficient information security management that includes a proper ISM policy (P10).

Secondly, the introduction of GDPR has put pressure on services providers throughout all areas to uphold the protection of citizens' individual data. Which in healthcare of course also entails that the data must only be processed for the purpose defined at the time of collection. The question is how to assess that this is ensured throughout the healthcare process. This too relates to how to set up and manage access (P05, P09). Thirdly, another aspect of the challenge of regulatory compliance is the lack of standards. For example, with the increase in mobile devices patients are also more likely to access PeHS on those devices, which presents other security challenges than with ordinary devices. This then leads to PeHS providers having to implement other security controls, but there is a lack of privacy and security standards that consider these types of devices (P13).

5.1.4 The users

As described by a few publications from the literature review, when dealing with PeHS one must consider the users as a considerable challenge both to information security and privacy. This includes both the users within healthcare (e.g., nurses, physicians) and persons in society (e.g., patients and private individuals). The first perspective for this challenge is formal patient consent, which is a highly debated topic within research. Some consider formal consent as unnecessary and that it is most beneficial to regard the patient's consent as automatic, especially within the same healthcare organisation. That is because the use of restrictive access due to lack of consent could negatively affect the patient's care if a caregiver is not provided with the necessary information. With that in mind, if the patient would like to specify that their information should not be transmitted to another healthcare provider that is acceptable (P05). The question here is how to handle the trade-off between formal consent and the convenience of wider access (P14).

In addition, patients might not even know what information of theirs that is included in PeHS and could be shared with other caregivers (P08). Although, as described by P17, some caregivers believe that their patients trust them to handle their data with care and do what they need to do to ensure the confidentiality of the data. Moreover, P10 describes that one of the primary challenges and threats to information security and privacy related to PeHS is the behaviour of the users. The users are unpredictable and could, both intentionally and accidentally, behave incorrectly in their data use and management which could lead to e.g., information disclosure. Another perspective is also the fact that the personnel within healthcare institutions are characterised as constantly interchanging staff, which puts strains on upholding the competence level regarding information security and ensuring an appropriate access level within the personnel (P01).

5.1.5 Applications

Next, there is the challenge to manage information security and privacy concerns due to the variety of applications involved (P18). Modern eHealthcare includes components such as mobile devices, sensors, Internet of Things (IoT) and medical devices with their own characteristics, requirements, and security vulnerabilities. For example, the different connected devices are also network connected and can therefore be exploited by an attacker. Once the attacker has exploited the device access to the organizational network or PeHS could be gained, and further damage could be caused such as attaching malware to the available data (P02, P04, P13). Moreover, the vulnerabilities of patients accessing the PeHS from their smartphones is a challenge too, since that also puts pressure on how the service applications are designed, accessed, and secured (P15). For example, what healthcare data could an unauthorized person access if they got hold of another person's smartphone? (P13)

5.1.6 Threats

The value of health data has made healthcare an attractive target for attackers (P15). Moreover, with the increased accessibility and usability the attack surface for eHealthcare has broadened and with that, there has been an increase in threats (P02). Therefore, this challenge is comprehensive and includes the many

different threats to PeHS. Such as the threat of unauthorised use, which relates to both ISMS and privacy (P03, P15). Some researchers focus especially on the situation of the patient data being shared outside of the eHealthcare environment (P15). While others emphasise insider threats as a great threat to the available patient data in eHealthcare and describe these as much more troublesome than any type of outside threat (P01, P04, P16).

Then there is the perspective of how to secure the networks on which PeHS is utilised, one being the medical internal network of the caregivers and the second one being the private networks of any other type of user. Since the data in PeHS are shared across these networks an attacker could use different types of attacks to gain access to that data e.g., eavesdropping, man in the middle attack or spoofing (P02, P09, P12, P13). The fact is that there has been an increase in cyberattacks over the last years and that is a threat to both information security and privacy because cyber-attackers could lock down entire healthcare environments hindering patient care using e.g., ransomware (P11, P18). The threats are not only troublesome from the perspective of an outsider gaining access to the data, but also the chance of data tampering which could lead to the wrongful treatment of the patient based on incorrect data (P03). Or data loss because of a malicious attack (P16). Lastly, another type of threat is the one of secondary data use by the caregivers with access to patient data. For example, the collected data within or about a particular illness could be used to gather data on a national level and in a national database. The data that one patient shared through PeHS in their own region could then be accessed by attackers if the national database is compromised (P01).

5.1.7 Culture

This challenge relates to the difference in cultural views of privacy and the consequences of that difference. These differences are especially obvious on a global scale. The challenge here is then to account for such differences and try to find a balance between sharing data to save patients' lives and protect the patient data with stricter access control (P14). Moreover, this challenge also includes the lack of a proper information security culture. The consequence of this is an increase in threats due to employees' misbehaviour and improper management of information (P10, P05).

5.1.8 Data lifecycle management

Since data transitions throughout its data lifecycle within healthcare and since it is shared among several parties one challenge is the data lifecycle management (P08, P17). For example, there are threats related to the data at transit since this involves the data moving across networks and devices (P13). Moreover, the data at rest or data storage is vulnerable to threats such as malware, hackers, or file-sharing tools. This stage of the data lifecycle has historically not been discussed within eHealthcare research. The challenge here is that there is a need for modification of security measurements due to the unique operational and compliance requirements within eHealthcare (P15). Furthermore, this grows more complex when discussing centralised versus local storage of healthcare data since it affects the privacy of sensitive patient data (P16).

5.1.9 Knowledge

This challenge is compromised by two areas, one being the internal knowledge within healthcare and the other being patient knowledge. A challenge with eHealth is that the involved staff is not provided with enough training on rights and responsibilities for both the staff itself and the patients. This includes both training regarding security and privacy (P15). This can slow down the development and implementation of appropriate PeHS due to a lack of knowledge in the relation to privacy and legal matters (P14). Researchers have also stated that there is a lack of comprehensive studies of the overall eHealthcare system (including the data, devices, networks, and processes). Hence, there is a lack of knowledge into how security and privacy could be ensured throughout the whole system (P02). Moreover, a challenge is the medical staff's lack of knowledge of what laws and regulations they must follow. For example, what GDPR entails and how that affects what or how information could be shared with third parties (P05).

Also, since the employee in most research is regarded as the weakest link in ISM, the challenge is to achieve a proper level of ISM awareness (P10). An example of this is that respondents of a focus group study declared that it is not their job as nurses to concern themselves with physical security concerns and that they themselves do not understand cybersecurity enough to understand the issues related to cybersecurity (P17). Since a lack of ISM awareness can increase the information security risk throughout the use of PeHS effort must be put into ensuring that the employees understand what ISM means and how their actions could compromise the security (P10). Lastly, from the internal perspective of this challenge, there is the issue of information practises. Without proper information practices, patient digital privacy could be violated and therefore the challenge is to implement information practices that ensure the least intrusive, identifiable and disclosure of sensitive information to as few people as possible (P08, P18). From the perspective of patient knowledge, researchers have found that a challenge is that with a lack of patient knowledge into the security and privacy risks the more vulnerable the PeHS is. Therefore, the best choice is to apply security and privacy by design for any patient accessible service such as patient portals (P12).

5.1.10 The technology/design

The tenth challenge relates to the choice of technology and design for PeHS. Firstly, there is a challenge relating to the design and development of dynamic and flexible PeHS. Because of the complexity and effects of eHealth services it is vital that end-users are involved in the development of the services. Both in the front-end design, but also functional design. Which includes both the patients and caregivers. Otherwise, the adoption and positive impact might be haltered (P12, P14).

Another aspect to this challenge is cloud technology. As a relatively new technology, cloud computing has been described as the future for easy data access and a good fit for healthcare since it promises e.g., solutions for more effective collaboration, communication, and coordination between different parties. However, there are aspects to cloud technology that have led to healthcare providers holding off on adopting the technology. For example, there are security risks such as identity theft, privilege abuse, and poor encryption (P06, P08, P09). Moreover,

the lack of standards and regulations for appropriately managing information security and privacy concerns are also obstacles for the adoption of cloud technology within healthcare (P01, P09).

5.1.11 Data characteristics

Because of the complexity and requirements of healthcare one must consider the data characteristics when dealing with data within healthcare. For one, there is the sheer volume of data to consider and the fact that more and more data is collected throughout the healthcare process. So, there is a challenge related to maintaining and managing the large amount of data (P06). Then there is the challenge of upholding the integrity and confidentiality of the data throughout the whole healthcare process (P01). While simultaneously preserving the data origins (P06). Lastly, a reasonable question to ask in relation to PeHS and the characteristics of the data generated about patients is what and how much data that is appropriate to share in PeHS since so many different people can access the data (P08).

5.1.12 Interconnectivity

This challenge relates to the fact that PeHS involves a multitude of different caregivers such as hospitals, primary care facilities, clinics etc. Because of this the interconnectivity has grown complex and will remain so as the need of access will increase, which is what PeHS providers must take into consideration (P02, P03, P04, P17). The security situation for PeHS is difficult to manage as the number of connected parties increase, the accessibility requirements, and the way of accessing the services increases. Moreover, to design and implement privacy policies for these services are challenging (P04, P06). In collaborative eHealth environments such as PeHS the parties involved range from authorities to individual caregivers, which leads to a constant high number of security weaknesses and patient privacy threats (P12, P16). The challenge is therefor to ensure that each of the contributing systems connected to the PeHS upholds the security standards, which will help ensuring the total security level of the interconnectivity between the involved parties (P07). For the development of future eHealth services, a challenge is also to design the infrastructure to be effective, safe, and secure (P11).

With many involved parties, a relevant question is to ask how the ownership of the data is assigned, which relates to data privacy. Normally the data owner is the creator of the information, which would make the patient the data owner of its own data. Which then indicates that it is the patient's choice of who to share that data with, even in an interconnected digital environment. To establish the data owner is essential to better protect again data misuse and unauthorized access (P09). Although, since sharing data only increases and the fact that the data is both stored and shared over several networks the data owner no longer have control over the data (P06). Which then leads to the question of responsibility of ensuing the level of security and privacy of the data, and unfortunately, there is no straightforward answer to that question as of now (P14).

5.1.13 Security practices

The last challenge relates to the applied security practices to ensure information security and privacy in PeHS. Several publications describe the challenge and

need for proper auditability of eHealth. To set up and run through audits of for example the most common system errors or activity records can become troublesome when dealing with larger systems used across multiple healthcare providers. With this, there is the challenge of upholding accountability for the safety and proper use of the available data when it is shared among several parties (P01, P15, P17).

5.2 Results of the Qualitative Interviews

The results of the qualitative interviews are presented below according to the categories that were identified during the data analysis. As presented earlier, a total of three categories were found and these categories relate to a variety of aspects regarding ISMS and privacy in general but also in relation to PeHS.

5.2.1 Sound prerequisites

As for the introduction of GDPR, all three of the interviewed respondents agreed that this put a spotlight on both information security and privacy throughout the organisation. Which was regarded as positive since it led to increased attention to information security throughout the organisations (R01, R02, R03). As respondent R03 explained, it started off with somewhat of a panic since people grasped the gravity of the situation once GDPR had been implemented and at that point, they were already in breach legally:

"*Yes, so it actually started with a fairly extensive panic when it was realised that the GDPR had already been introduced and that we were by definition illegal.*" (R03)

Respondent R03 also described the nature of the work with GDPR as constant and that they are still experiencing challenges concerning the handling of issues related to GDPR. Moreover, as respondents R01 and R02 discussed, the implementation of this regulation opened peoples' eyes to information security work in general, and it also increased the level of competence and knowledge in this area:

"[...] this meant that efforts were made to introduce it and that the focus was on this area and the information security work in general. Which is very positive, I think, and we who work with information security. It's on the agenda. So there the eyes were focused on the processes we have in information security and that was positive." (R01)

"[...] it really made the organisation work intensively with these issues and then brought them up on the table and increased the competence and knowledge level within it as well." (R02)

In addition, when asked about the ISO standard ISO/IEC 27701 that was produced to help understand the regulation a distinct difference between region A and region B was identified. Respondents R01 and R02 from region A described that this standard assisted to link the work they already did with other standards in the ISO 27000-series with GDPR, without having to work with GDPR on a separate track. However, in comparison, respondent R03 from region B explained that they had not been applying this standard at all:

"It makes it easier because it somehow still clarifies how you can think, how you can work. And above all linked to GDPR, I felt that it was helpful that the standard came that pointed to the work that we are already doing within the framework of 27001 and 27002 then you need to dock this from a GDPR perspective, [...] it is integrated into the already existing work." (R01)

"I'll be completely honest. We have not looked at it that much because we are swamped in the GDPR problem." (R03)

Respondent R03 also explained how they in their region have made progress with the healthcare staff in relation to PeHS. This region has been involved throughout the process of developing and implementing Journalen, they have also mapped the information flows and how to properly build the security for the platform. This included performing risk assessment in different areas and with different situations in mind, such as end-user behaviour and relation to e.g., social media. Moreover, this region has made progress regarding their ISMS in relation to PeHS from the perspective of the employees' comprehension of the consequences of this type of service:

"We have been involved and there has also been a dialogue with healthcare institutions. Some have been very sceptical, such as psychiatry for good reason. [...] So yes, we have thought through it really well. And we have now also got healthcare staff to accept this, and it was a struggle." (R03)

In addition, respondent R01 described that there is a general challenge for the Swedish regions to get their information to their healthcare personnel about the PeHS that the region provides. This also includes what routines that apply in relation to the PeHS:

"There is a challenge in all regions to reach out with information to healthcare professionals about services used by patients/citizens. Our region has good information for employees, but we can become even better at taking the time to update ourselves on what applies and ensure that new employees are informed about current routines." (R01)

Also, respondent R03 added another perspective to the challenge of healthcare personnel's understanding of PeHS by describing an issue that their region had found where the healthcare professionals have started changing their behaviour in a negative way and input information in the incorrect field in the medical record system:

"Healthcare professionals are aware, and they have now begun to express themselves in a different way in the medical record system so that it is understandable to the patient, but then they instead use the comment fields in the medical record system and that is not good either." (R03)

Another important aspect is the citizens' understanding of the PeHS and their own behaviour when using these services. When asked about challenges with user behaviour related to the use of PeHS respondent R03 described that there are challenges related to the citizens' and patients' behaviour. Respondent R03

talked about how Facebook groups are created by employees and then utilised by citizens to ask questions:

"[...] there are some Facebook groups [...] where the Facebook group is actually started by employees, but it looks very official. It has happened then that citizens ask questions about their illnesses in the belief that it is some kind of PeHS." (R03)

When the respondent was asked about how this, and other challenges are managed by the region respondent R03 described that there are instructions presented to the citizen or patient when they log into Journalen and that the hope is that they read through those before proceeding to the next page:

"[...] when you log in to 1177, you get a lot of instructions to read, what it means to use these resident services and then you have to press the little button that you have read the information. [...] But it's clear there are sure people who just click hello wildly in the usual order, but we have tried to do what we can" (R03)

Moreover, the respondents from both region A and B expressed that there is a challenge to get the organisations to understand what information security entails and how they should work with their information security, which in turn is a challenge to the ISMS (R01, R03). This includes both the actual reason behind the need to perform certain tasks within the information security work and what tools that are available to them within the region:

"[...] to also understand why we have these methods. Why do we want you to analyse, because it actually benefits you who are responsible for the information. [...] and then you have the help of these methods and tools to be able to achieve it [suitable information security]." (R01)

"It is to get the organisation's understanding of how information security work is conducted and what tools are used and why. That is the challenge, I would like to say. [...] but now the understanding begins to fall into place and then you can use management systems and refer to it." (R03)

When discussing how the threats to PeHS affect the region's ISMS and privacy respondent R01 described that it absolutely affects their systematic information security work. Moreover, what this comes down to is that the employees working with the ISMS must understand the prerequisites and requirements to be able to provide a suitable management system and tools to secure PeHS:

"It's the cornerstone. If we are to be able to meet the outside world, if we are to be able to meet reality, we must understand the needs that exist, the threats that exist, the aspects we need to take into account in order to be able to adjust in our systematic information security work to make it as effective as possible." (R01)

Lastly, an interesting aspect brought up by respondent R03 when asked about what the biggest challenges for PeHS are in relation to their region's ISMS and privacy, the respondent described that health care personnel can get a bit carried

away and want to implement inappropriate services. Thereby, a challenge is to understand and ensure that the desired service has a real benefit to the patient:

"One challenge is to try to have a sensible discussion about whether the service actually provides the patient with any real benefit. Usually it does, but sometimes there are some a little too crazy ideas that you have to resist." (R03)

5.2.2 The processes

Respondents from region A emphasised repeatedly during the interview that structure and standardisation would assist them in their information security work and to design an appropriate ISMS. Moreover, they pointed to the help it would lead to if there was a national direction that the regions could lean on regarding the related legislation (R01, R02). Respondent R01 also described that the use of standards such as the ISO 27000-series assisted them in their work to achieve an appropriate ISMS:

"[...] everything that is a standardised basic platform makes it easier and that is also how we have chosen to apply the ISO 27000-series as an aid. So, I would say that it facilitates our work. Then the challenge is that there are many standards that we were on before, but there is also a very good work in general that they are compatible, and they are so general that it is possible to have different types of frameworks that still work together." (R01)

What the respondents all described in relation to different questions during the interview was that there is great complexity to the relation between ISMS, privacy concerns and PeHS. This complexity is the result of different aspects (R01, R02, R03). For one, the respondents pointed out digitalisation as challenging, both from the perspective of keeping up with the needs of the organisations and the threats that the digitalisation leads to:

"So, it is a challenge to catch up with the development that is taking place. Especially when we talk about connected to patient-centred services and the type of digitization that a patient-centred care requires and that the patient is in focus, and so on." (R01)

"[...] the more digital we become, the more vulnerable we become. Both on the basis that those who do not have access to information get access to it. On the basis that the information is not correct or incorrect and when you talk about several attack surfaces and the like, we know with us, with the world situation that we now have as well." (R02)

Another aspect that makes the situation complex is that legislation in connection to information security and ISMS itself do not keep up with the digitalisation, which greatly affects the ISMS work:

"I also think in terms of legislation, so we also see that it will come, what can you say, a little later. [...] Which means that then we have developed things based on current legislation, we need to go back and redo. [...] And we always need that in all activities, but here there are already many technical components involved." (R02)

Moreover, the respondents also pointed out that the increase of mobile devices of different types also complicates the security situation:

"In general, if you look at it from an information security perspective, the more units we have, the better we need to ensure information security all the way out [...] it's like what reality looks like and that's what we need to work on to keep up with the pace of development because that's what reality looks like." (R01)

"I think that is a problem for all companies. [...] mobile devices are a black hole." (R03)

Also, respondent R01 described the complicated task of finding a balance between all the different perspectives that influence the design of ISMS and the use of ISMS. This includes legislation, organisational point of view from different organisations, technology etc. All these perspectives must be added, examined, and adjusted to provide the best service:

"We need to work systematically with our information and the security work linked to it. And that means that we need to do quite tricky analyses sometimes and especially when it comes to services that have a very large business benefit. It is important that the balance is very clear, that you get all perspectives and that the processes ensure that we get the information security work and the perspective of information security/data protection when we introduce and when we manage." (R01)

Moreover, respondent R03 touched upon the challenge of responsibility of ensuring that information security/data protection is handled in a satisfactory manner in relation to PeHS:

"If you look at Electronic Health Record data, for example, we use the system Cosmic, then it is the administration that is responsible for transferring data but then the data needs to be received and there I am not entirely sure that the interfaces are completely defined." (R03)

Next, for the ISMS process, respondent R02 described that again that there are challenges related to keeping up with the digitalisation, and even though the region deems that they have a good basis to work from they still have a lot of work left. Respondent R02 also made an important comment about the fact that with the ISMS process you cannot set a goal that indicates that there is an endpoint to the process, because the process is continuous and always in a state of change therefore there is no endpoint. Furthermore, respondent R03 stated that a challenge to the ISMS process is to identify information assets e.g., medical technology systems handling personal data that flow around:

"But then there is the problem of identifying sources of information and then making sure to classify them and take action based on any leaks or legal problems." (R03)

As for the tools applied, both regions A and B do utilise the ISO 27000-series to some extent (R01, R03). Furthermore, when asked what could be improved with

the methods and tools used for the ISMS work respondent R01 did not identify any direct points of improvement with the tools or methods. However, the respondents had previously described that the tools and methods are generic and general and need to be adjusted according to the organisation applying them(R01). The points of improvement with the tools and methods lay more with the people applying them:

"It's a craft. It requires the laying on of hands. It takes time. It requires skills development. It requires that we learn from each other and that we learn from those experiences to become even better." (R01)

Furthermore, when asked if the tools and methods available in the region can be applied to PeHS respondent R01 clearly explained that there is no difference between services. No matter the service the tools and methods should be applied Also, the introduction of new PeHS follows the same qualitative implementation process:

"[...] the methods and tools are generic and general, so they must be applied regardless of service, regardless of the type of information." (R01)

One point of discussion during both interviews was related to access privileges and the responsibility of managing the access privileges related to PeHS. Respondents from both regions described that a trade-off is made between consent and access privileges in emergencies since this in fact could be detrimental to the patient's life (R01, R03). Moreover, the responsibility of making sure that the access privileges to PeHS are correct lies with the managers, which also must be improved for in situations such as when employees change work duties within the organisation yet keep their old access privileges (R01, R03).

5.2.3 Possible collaboration

The respondents identified several opportunities for improvements for ISMS and privacy related to PeHS during their interviews. For example, as for the positive influence on user behaviour when using PeHS respondent R01 described that the region needs to be more visible in their information, education and dialogue with both citizens and healthcare personnel:

"Through information, education, and dialogues. As a region, we need to be "out" and visible where both residents and care staff are. We need a "kiosk" to inform about PeHS at e.g., the region's hospital, we need to be seen at the patient association and more." (R01)

The education regarding information security could also be updated so it covers more aspects related to PeHS:

"Just social media, that passage also exists. But not explicitly when it comes to PeHS, but that you should not answer any questions and preferably delete those that may be to the detriment of the patient or the resident. So, it's a challenge." (R03)

Moreover, there is room for improvement regarding the related legislation and the standards which would positively affect the ISMS process:

"[...] sometimes it is not the case that the legislation points in the same direction, they can even stand directly against each other, and in addition, we have our mission to create the best conditions and provide the best care to the patient." (R01)

"It is absolutely stilted [ISO standards]. It is not necessarily easy to understand. [...] ISO standards are very tedious." (R03)

Lastly, one aspect of the challenges regarding ISMS and privacy is that each Swedish region is dealing with some of the same issues, risks, and challenges but the options of collaboration between organisations and other regions are limited:

"There is, of course, regional cooperation in some parts, but ultimately and apparently, we are individual authorities with responsibility for our own information. And we can never, as it were, transfer risk ownership to someone else, but here it is a matter of based on the consensus that can be created nationally, everyone needs to go home and think about what risks we are willing to take based on the conditions we have in our organisation." (R01)

5.3 Analysis of the joint results

Common denominators between the results of the literature review and the results of the qualitative interviews conducted during the thesis work have been identified. For example, both results have included a theme related to knowledge. This corroborates what was initially found in the literature review, there is a need to improve the knowledge of ISMS and privacy, both generally and in direct connection to the use of PeHS. Moreover, this lack of knowledge or need for greater knowledge is not limited to just healthcare personnel or patients, all end-users of PeHS need greater knowledge on how to securely handle the available PeHS.

Furthermore, the joint results also indicate that there is a great challenge to ISMS and privacy simply due to the characteristics of healthcare. There are several parties that must collaborate and integrate for the healthcare services to be effective. This is challenging both from the perspective of multiple stakeholders that need to collaborate, but also because of the differences in their systems and IT infrastructure. Also, besides all its benefits, digitalisation presents a great challenge to ISMS. This is because digitalisation develops faster than what the adjustments in the ISMS are implemented and that there is an increase in both services and mobile devices that need to be taken into consideration.

As for the challenge of access control, there are multiple aspects to consider. Some aspects could be interpreted as easier to deal with considering the results of the qualitative interviews, such as the issue of should versus must have access from the perspective of emergencies. Both regions represented in the interview study have made a distinction regarding the access privileges assigned to the emergency departments, which is based on the potential of patient harm or in the worst-case scenario even patient life. Therefore, the emergency department personnel have high privileges.

6. Discussion

The sixth chapter of this thesis report is dedicated to the discussion on the work conducted in comparison to previous research and the application of the data collection and data analysis methods. This chapter also presents an elaboration on ethical and societal aspects related to the thesis work.

6.1 Previous Research

There are similarities between the results of the thesis work and the related work presented earlier (see chapter 2.2). For example, Mense et al. (2013) found during their study that there is a chance that organisations misunderstand the concept of information security and interpret it as requiring mainly technical security controls. This is reflected in the joint results of the thesis work since the theme of knowledge was identified in the collected material. The results of this thesis work include the employees' understanding of what ISMS entails, how the tools and methods of ISMS should be applied, the consequences of user behaviour and in relation to PeHS specifically there is a lack of knowledge on how to ensure the security and privacy of the whole healthcare system chain.

Moreover, Jara & Schafir (2014) pointed out in their study that there is an additional security requirement concerning information security that must be taken into consideration. This too is reflected in the results of the thesis work and that this is something that must be improved, for example, the managers that are assigned the responsibility of keeping the access privileges up to date must actively fulfil this task throughout the employees' time in the organisation (e.g., remove privileges when the employee is assigned other duties).

In addition, the interview respondents confirmed the need for a dynamic ISMS that can be adjusted depending on the organisation and situation in hand, which was something that Mense et al. (2013) also presented as important. Another similarity to the results of the thesis work is what Amankona et al. (2021) presented regarding the necessity to implement appropriate policies, guidelines and regulations in order to mitigate security and privacy issues related to eHealth. This too was emphasised in the results of the thesis work, but also the difficulty of doing so when the legislation contradicts one another, and standards are sometimes difficult to fully understand.

Also, Scandurra et al. (2017) explained that healthcare is a complex organisation and it is difficult to manage since several different actors have to collaborate within the same space. Moreover, Scandurra et al. (2017) also identified that there was a gap between the legislation at that time that effected PeHS, which also was found in the results of the thesis work. A difference on the other hand is what the results of the thesis work did not indicate regarding a resilience to develop eHealth services which was presented by Scandurra et al. (2017). The interview respondents did not answer any question to that effect and there was nothing obvious in the literature review that indicated a resilience to develop eHealth services. Though, perhaps an interpretation could be made in relation to the new technology (e.g., cloud), which was identified as challenging to adopt in the development of new PeHS in the literature review results.

6.2 Personal eHealth Services

One of the obstacles encountered during the thesis project was to interpret the concept of Personal eHealth Services. This is a new concept mostly used within Scandinavia. The concept is only found when looking at the research project description provided by *NORDeHEALTH* (2022) and as it is referenced by *DOME* (2022). Because of this an interpretation of the concept had to be made to determine what services that count as PeHS although they have not been categorised as such in the literature. For example, EHR is not found to be a PeHS since EHR is simply the transformed version of health records being digital instead of the traditional paper-based records. Although, with EHR there is possible to offer PeHS in relation to the medical records. The most apparent services that could be included as a version of PeHS is Patient Accessible Electronic Health Records simply due to its characterisation as patient accessible. In addition, PeHS also include services that for example allow for web-based contact with the healthcare providers (e.g., to book appointments or renew prescriptions). In essence, from working with the concept, the interpretation is that there are more services of this type available in practise and described in literature, but they have not been categorised as PeHS since the concept is new and not broadly applied within the research area.

This made it difficult to find literature that describe the concept in general for the background chapter of the thesis report and to identify publications relevant to the systematic literature review. For the literature review, the lack of publications applying the concept affected the search terms for the review. Since so few hits were found when using more specific search terms (including PeHS) the search terms had to be redefined and less specific to allow for a satisfactory number of search hits. For example, the broader search term combinations included terms such as record (would thereby include EHR) instead of targeting the potential literature by simply using the search term PeHS. In fact, none of the previous works presented in the thesis report or publications included in the literature review mention PeHS. They do however describe characteristics of PeHS for services that allowed for them to be included in the thesis work.

6.3 Research approach

As described by Almeida et al. (2017), no matter the characteristics of the research topic and method, the research could experience limitations related to the research process. With this thesis work, the planned work was ambitious with the time limitation and limited resources. Apprehensions were also communicated to the supervisor and representative from DOME early on during the thesis work related to the available and applicable publications for the systematic literature review. To mitigate this potential limitation the research method and process were chosen with care and designed to utilise different database resources as recommended by Kitchenham (2004) and Brereton et al. (2007).

Thereby, which is also reflected in both the analysis and results of the literature review, a trade-off was made between applying broader search terms to allow for a larger number of search hits in exchange for putting more pressure on the time limitation. This choice proved to be positive in the sense that most of the accepted publications did originate from the broad search term combinations, but

it was not as positive as wished for since the broader search terms proved to be less effective than expected since so many publications did not fulfil the selection criteria.

In addition, apprehensions regarding the plan of conducting both a comprehensive systematic literature review and qualitative interviews were discussed with both the thesis project supervisor and a representative from DOME, which again had to do with the time and resource limitations. However, it is recommended to apply more than one method when available in qualitative research to broaden the data and not rely solely on one source (Arksey & Knight, 1999). Because of this, qualitative interviews were conducted after the systematic literature review to compare, corroborate, or differentiate between challenges found in research with challenges managed in practice.

Although, the primary data collection method was the systematic literature review, and the addition of qualitative interviews was viewed as complementary but not necessarily required for the thesis work. This is also why it was acceptable to conduct only two interviews even though the plan at the beginning of the thesis work was to conduct up to six interviews.

6.4 Review process

The systematic literature review process applied during this thesis work consisted of several steps in three phases (see Figure 4) and control points with both the supervisor and representatives from DOME. The first phase of the review process was initially uncomplicated and rather easily conducted, included in this phase was the choice of database resources, the definition of search terms and the definition of selection criteria. Since the thesis work was done as part of a larger research project tasks such as defining search terms and database resources were made easy since some work had already been done by DOME.

However, the selection criteria took some more work. For one, it was found during test searches that the number of search hits greatly overpassed the possible number to review for the thesis work. Because of the large number of search hits the inclusion criterion for publication date was changed from ten years to five. Although, even with this action the search hits were considerable, and it took more time than expected to filter through the search hits. Moreover, defining the selection criteria to ensure that publications of high relevance and quality were included and at the same time excluding those publications that did not meet the necessary level also took more time than anticipated.

The second phase (see Figure 4) included the steps for conducting the review. When executing the database searches with the search terms the initial collection consisted of 18, 668 search hits, which needed to be processed according to the selection criteria that had not been applied during the database searches (e.g., eliminate duplicates). For this process, the choice was made to not utilise any form of reference management tool, partially because no reference management tool had been used this purpose previously in earlier projects and it was not deemed that using a reference management tool was necessary. Because of this, the publication details from the search hits were documented in an Excel sheet and then processed the publications manually in Excel.

The selection process was more time consuming than expected, but that was found to be caused by the sheer number of publications to process and not any lack of functionality in Excel or the fact that the files downloaded from the different database resources which included the publication details also varied in their format and detail. For example, much time was spent extracting the relevant publication details from the downloaded file after each database search and then pasting that information into the Excel sheet. Because most of the selection process was done manually (reading row by row to determine e.g., if the publication was a duplicate based on the title) a satisfactory overview of the collected material was achieved. Once this had been done a total of 17 valid publications had been accepted. At this point, the backwards snowballing process began, which was utilised to backtrack and identify other potentially relevant publications that had been missed during the database searches. The snowballing process resulted in another 1,060 possible publications being processed according to the same procedure as before and after completion, one more publication was accepted. Again, this also was time-consuming.

In the end, out of the total 19,727 processed publications 18 were accepted for the data analysis. The final number might seem low in comparison to the large number of publications found through the database searches and backwards snowballing process. An explanation for this lower number could be that the search terms were quite broad. Looking at the statistics presented in Table 5 the narrower search term combinations did not result in many hits, which could indicate a lack of research into the area that those search term combinations targets. Moreover, most of the excluded publications were excluded because of their lack of relevance to the thesis work (e.g., medical focus and perhaps only mentions of information security or privacy). Which was primarily done by reviewing the publications' titles.

Also, the goal of the selection process was to eliminate as many irrelevant publications as possible to limit the number of publications to read in their entirety. Thus, an exhaustive approach was adopted during the selection process. Apart from eliminating publications based on an assessment of their title to determine relevance, publications with results that were dubious or difficult to grasp due to inadequate description of results were also eliminated. Thus, there is a possibility that some disqualified publications could contain relevant information concerning challenges relating to ISMS and privacy regarding PeHS. With more resources, a logical choice would be to perform a closer initial assessment which would perhaps lead to more accepted publications. Moreover, due to the literature review taking longer than expected the analysis of the literature review was delayed, which in turn also delayed the design of the interview guide. Consequently, less time could be allocated to interviews and that might affect the possibility of booking more interviews.

6.5 Interview process

The process for the qualitative interviews started early on during the thesis work since it involved the collaboration with a representative from DOME. The potential sample selection was discussed along with the potential number of interviews to conduct. A couple of weeks into the literature review dates were set for the interviews to be planned and from that point, the representative from DOME

started reaching out to book interviews. However, getting participants for interviews became one of the greatest issues for the thesis work. Perhaps this could correlate to the time and situation in the world, and because of that, there might have been less of an interest to participate in the study even though it might have been regarded as relevant for their organisation.

Moreover, as explained above, the process of designing the interview guide was delayed due to the prolonged literature review process. Therefore, less time was available to conduct interviews. The goal was to conduct six interviews where the participants would come from a mix of regions and preferable roles such as DPO or CISO. In the end, two interviews were conducted and only one of the three participants described themselves as a CISO. The other two participants described themselves as competent and directly involved with the ISMS work within their region. Also, all three participants felt comfortable answering the privacy aspects of the interview questions as well. Once the DOME representative had gotten confirmation from a participant and booked a time for the interview, the participants' contact information was forwarded to the interviewer who contacted the representative with a short presentation of the thesis project, the purpose of the interview and a Zoom-link for the upcoming interview. Also, a day before the individual interviews the interview questions were sent to the participants. This was done to ensure more comprehensive answers during the interviews and to reassure the representatives about the topic of the interview.

At the start of each interview, the participants were asked about approval for recording, which all agreed to. The third participant did require that only the interviewer would review the recording and once the material had been transcribed the recording would be deleted. This was not seen as a problem for the thesis work and was therefore accepted. Next, the participants were asked about approval to name their organisational affiliation and region in the thesis work, but since one of the participants wished to not have any identifiable information about themselves or their region in the thesis work a decision was made to only declare the participants' roles in the thesis work. Therefore, name, organisational affiliation and region are all anonymised in the thesis work throughout. After all the approvals had been covered the participants were again informed about the thesis project's aim and purpose of the interview, during which an emphasis was made that the collected material from the interviews would later also be used in the larger research project conducted by DOME. After these steps, the interviews were conducted following the interview guide. Once the interviews had been completed the participants themselves asked for the chance to check the collected material once it had been transcribed before sharing it with DOME and the thesis report before publication. Again, this was not viewed as an issue since it increased the trustworthiness of the thesis work.

After the interviews had been conducted, the recordings from the two interviews were both transcribed within two weeks and sent to the corresponding participants. At this point, another issue became apparent, because the participants did not reply. It required several follow up emails before replied. A couple of days after the transcribed material had been sent out one of the representatives got in contact, but at that time could not approve the transcribed material and asked for more time to review it with a colleague. The participant from the second region did not respond to any emails until the final attempt two weeks after the

follow-up message had been sent originally. Luckily, all participants signed off on the transcribed material which allowed for the thesis work to continue. This waiting period did cause some stress, but since the participants approved the material in the end there was no serious consequence to the thesis work.

6.6 Analysis processes

Two methods for analysis were performed, thematic analysis for the material collected during the systematic literature review and qualitative content analysis for the material collected during the qualitative interviews. Both analysis methods were familiar from previous projects, but they took considerable time to utilise due to the characteristics of the collected material. Firstly, to code the material from the systematic literature review efficiently, systematically, and correctly was difficult because of the varying level of language. This proved to be both time consuming and required several iterations of reviewing the potential themes that were identified through the grouping of the codes. Secondly, the analysis of the interviews proved to be difficult because of the limitation of material. Therefore, it took more time than anticipated to identify all the relevant concepts and define the codes, categories, and themes for the qualitative content analysis.

Moreover, initially, the plan was to perform a high-level analysis for the systematic literature review but upon beginning the analysis it was decided that a more comprehensive analysis of the accepted publications would benefit the thesis work. Therefore, a decision was made to conduct a detailed thematic analysis. This decision also made it more apparent that the primary data source for the thesis work was the publications found during the literature review and the results of the review would be the primary result of the thesis work. Although, correlating the results for the analyses proved to be straightforward and did not take as much effort as expected.

6.7 Results

As presented earlier, the thesis work was expected to provide a taxonomy of challenges in ISMS and privacy related to the use of PeHS. With a taxonomy of challenges in this area future development of methods and tools for ISMS with eHealth services could be assisted. This was provided by conducting a systematic literature review in which 13 themes of challenges were identified and defined. Moreover, since the results of the literature review were utilised as the basis for the qualitative interviews the taxonomy was corroborated by respondents working with ISMS and privacy within two Swedish regions.

The results from both the literature review and the interviews could be interpreted as there should not be and is not a difference between PeHS and other types of services provided within healthcare. For example, as the interview respondents explained, the ISMS is general and although it might need some adjustments depending on the situation, it should be applied no matter the service or what information that the service manages. On a general level, the results can also be interpreted as identifying digitalisation as a great threat and influence on both ISMS and privacy, both in relation to PeHS and throughout the organisations.

The outcome of the thesis work is not specific to Sweden or only the two regions represented in the interview study. The results based on the literature review included publications published in English and in different journals or conferences, thereby the results were general. Furthermore, the results of the thesis work have been supported by the related work (see chapter 2.2) which also ensures the generalisation of the results. To further generalise the results more database resources and search combinations focused on information security and ISMS in relation to PeHS could have been applied, in combination with more interviews with several Swedish regions and perhaps even internationally.
The results of the thesis work provide an insight into how practitioners in this area experience challenges and what could be improved regarding ISMS and privacy related to PeHS. The results could also be used as a basis to perform in-depth studies focused on the challenges found in relation to ISMS and privacy related to PeHS.

6.8 Ethical and Societal aspects

As part of the discussion for this thesis work potential effects on ethical and societal aspects have also been included. These aspects are presented in two subchapters below.

6.7.1 Ethical

As described in subchapter 3.5, several ethical considerations have been taken during this thesis work. In relation to GDPR, no personal information about the interview participants have been documented and the audio and video recording from the interviews were erased once they had been transcribed. Moreover, the participants themselves have reviewed the transcribed material to validate that no sensitive information about themselves or the region they represented was included in the transcribed material. In addition, it should be emphasised that most of the results presented in this thesis work are a condensed summary of existing external research. Thus, the information drawn from that research is neither fundamentally new nor secret since it is freely accessible on the Internet, which of course includes any potential threat actors that might try to draw conclusions on how to exploit the challenges with ISMS and privacy in relation to PeHS.

Summarising and presenting identified challenges with ISMS and privacy concerns related to PeHS could help increase people's knowledge about the prerequisites of ISMS and privacy in this digital day and age of healthcare. This includes healthcare personnel, citizens and patients that have an interest in PeHS. Even though no mitigation solutions for the challenges are included in the thesis work the results are still deemed as beneficial. For example, it could help patients understand that healthcare providers social media does not count as a PeHS and therefore information shared over social media with a healthcare provider is not encouraged since the information security could not be ensured. This also applies even though a threat actor theoretically could find the results interesting as well. No further ethical aspects were observed during the thesis work and therefore the discussion on ethical considerations is congruent with the description given in chapter 3.5.

6.7.2 Research Ethics

Although the conducted literature review did not include many accepted publications focused on ISMS instead of individual information security challenges, the results of the review are still judged as comprehensive enough to be included in the mentioned research project by DOME whose aim is to complete an analysis of the information security and privacy perspectives related to PeHS. If it is found that there is a shortage of information concerning any area of interest, it can be collected by targeted research into that specific area. However, this does not render the work presented in this thesis worthless, instead, it can be viewed as a valid foundation in combination with additional data for the DOME research project. In addition, other research or even organisations might find the result of this thesis work applicable for gaining better knowledge into the challenges with ISMS and privacy related to PeHS (e.g., perhaps in the development of new PeHS).

Since threats to the trustworthiness of the thesis work were managed throughout the thesis project stages, the presented result was deemed as credible and could therefore be applied to other projects or studies. Also, the transparent and detailed descriptions of each applied research method during the thesis work allow for potential external researchers to replicate and thereby evaluate the performed work.

6.7.3 Societal

Both the conducted systematic literature review and qualitative interviews have been deemed to prove that there are challenges regarding ISMS and privacy concerns in relation to PeHS. Hence, the challenges are not only theoretical or excluded to Swedish regions, in fact, the Swedish regions represented in this thesis work have experienced some of the challenges identified in the literature review. Therefore, the results are beneficial to a variety of parties. These challenges are associated with a variety of aspects as presented in the results (see chapter 5) and help PeHS providers to get an overview of documented challenges related to ISMS and privacy concerns. The results of the thesis work could perhaps also be utilised as a basis for cross-region collaborations and discussions regarding the challenges related to PeHS. Moreover, the results of this thesis work might assist developers, administrators, and facilitators of PeHS in what challenges they should consider for future services, which thereby could lead to the challenges related to ISMS and privacy being mitigated even before the organisation approach the situation of adapting and providing the PeHS to their citizens.

Moreover, the conducted systematic literature review highlighted that there are challenges regarding ISMS and privacy concerns in relation to PeHS that are not characterised as technical issues. In fact, there are challenges related to e.g., legislation and human behaviour. By increasing the knowledge and understanding of these aspects, the thesis project can help PeHS providers to redirect some of their focus to the more intangible aspects of ISMS and privacy.

Furthermore, as described in the introduction of the report, there is a transition towards more patient-centred and transparent patient care. The patients of the digital age want to be more involved and has the potential to add to their own care since it is possible to gather, process and analyse so much more data about the patient's health as described by Nurgalieva et al. (2020). Therefore, from the

patient perspective, the PeHS must have a functional purpose and information about the available services must be properly presented to the citizens. However, the results of the thesis work show for example that the citizens do not have enough knowledge about the PeHS and therefore put their own sensitive personal information at risk due to improper user behaviour. Therefore, when developing future PeHS the providers must be mindful about what the citizens understand about the service, which functions that are available, what information that is transferred between the healthcare parties and how the citizens themselves must act to preserve the privacy of their information.

7. Conclusion

This last chapter is dedicated to presenting the conclusions of the thesis work. The conclusion has been divided into subchapters, the first relating to the performed analysis, the second relating to the research questions for the thesis work and the third relating to future work.

7.1 Based on Analysis

As presented in chapter 5, several challenges regarding ISMS and privacy related to PeHS have been identified both in the literature and in practice. Some of these challenges are general and some are specific to PeHS. For example, one challenge relates to the lack of understanding among the employees of why they should apply the methods and tools available to ensure the information security of their services. Moreover, one challenge relates to human behaviour among the users of PeHS. This includes both healthcare personnel and patients. For example, when learning what information is sent from the EHR system healthcare personnel might try to be clearer and provide easier information to understand since it is available to the patient through PeHS. However, in doing this they might also start using the EHR system incorrectly and add vital information somewhere in the system where it is not supposed to be documented.

On the other end, patients might misinterpret information or communication channels available through social media to get in contact with a healthcare provider. Thereby, they might unconsciously share private information about themselves because they have misinterpreted social media as an official communication channel with the healthcare provider. Lastly, reflecting upon the purpose of the thesis project. The purpose of this thesis project was to understand and describe the issues related to ISMS and privacy regarding the use of PeHS. The results presented in chapter 5 is deemed to fulfil this purpose since the results includes a multitude of perspectives and different types of challenges, which has been found both in research and in practice.

7.2 Answers to Research Questions

The first research question for this thesis work was aimed at identifying the challenges with ISMS and privacy in relation to PeHS, and both the literature review and the interviews revealed that there are several challenges to consider in this area. In total 13 themes of challenges were identified through the literature review, which was then corroborated by the interviews conducted with representatives from two Swedish regions. These challenges include a variation of aspects. Some examples of challenges are access control, patient trust, collaboration between multiple parties and lack of knowledge.

The second research question was aimed at identifying how Swedish regions are applying ISMS for their PeHS and how they are managing the privacy concerns. From the analysis of the interviews, it was found that the regions participating in the research project does not differentiate between PeHS and other types of services. Therefore, one and the same ISMS is applied to all services independent of its purpose if it manages personal information. Regarding privacy concerns,

the respondents expressed that their way of managing potential privacy concerns is to build privacy management into the ISMS. This is done by for example utilising standards focused on merging GDPR into the ISMS process, thereby the ISMS no longer simply focuses on information security but includes privacy aspects as well.

7.3 Future work

In this thesis project only two Swedish regions were represented in the qualitative interviews and therefore a natural future work would be to expand the research by involving more regions, which would provide perhaps even more general results. Moreover, a delimitation of this thesis project was to not provide any solution formulation to the challenges found regarding ISMS and privacy in relation to PeHS. Therefore, future work could be to use the results of this thesis project as a basis and present solutions to the identified challenges. This could be done in several ways. For one, the aim of the future work could be to target the challenges related to the more abstract aspects such as human behaviour and how to influence users in their information security behaviour. Another aim could be to focus on what aspects of ISMS could be standardised cross- regions and what that would require in the form of e.g., legislation, standards and tools for ISMS or privacy management.

Another delimitation was that no technical challenges such as technical setup were included in the thesis work. With that in mind, a possible future work would be to complement the results found in this thesis work with an analysis of the technical challenges regarding ISMS and privacy related to PeHS. By doing this it could be possible to perhaps link the challenges and from there develop an even greater overview of the challenges and their correlation. Moreover, as mentioned repeatedly in previous chapters, the thesis work will be included in a larger research project conducted by DOME. In that project, some of the work done for this thesis will be the basis for further data collection e.g., the interview guide will be used both nationally and internationally in the research project's interviews. This too could enhance the results and make them even more general.

Lastly, this thesis work did not include a patient perspective, a future work could therefore be to complement the results of this project with research focused on the patient perspective on information security and privacy related to PeHS. This could assist improving and ensuring the development of future PeHS since it would take both the providers' and the patients' perspectives into consideration

References

Åhlfeldt, R.-M., & Söderström, E. (2007). *Information Security Problems and Needs in a Distributed Healthcare Domain – A Case Study*. 97–108. http://urn.kb.se/resolve?urn=urn:nbn:se:his:diva-2109

Ak, B., Tanrıkulu, F., Gündoğdu, H., Yılmaz, D., Öner, Ö., Ziyai, N. Y., Erol, F., & Dikmen, Y. (2021). Cultural Viewpoints of Nursing Students on Patient Privacy: A Qualitative Study. *Journal of Religion and Health*, *60*(1), 188–201. https://doi.org/10.1007/s10943-020-01062-z

Alfawaz, S. M. (2011). *Information security management: A case study of an information security culture* [Doctorate thesis]. Queensland University of Technology.

Alharam, A. K., & El-medany, W. (2017). The Effects of Cyber-Security on Healthcare Industry. *2017 9th IEEE-GCC Conference and Exhibition (GCCCE)*, 1–9. https://doi.org/10.1109/IEEEGCC.2017.8448206

Al-Issa, Y., Ottom, M. A., & Tamrawi, A. (2019). eHealth Cloud Security Challenges: A Survey. *Journal of Healthcare Engineering*, *2019*, 7516035. https://doi.org/10.1155/2019/7516035

Almeida, F., Faria, D., & Queirós, A. (2017). Strengths and Limitations of Qualitative and Quantitative Research Methods. *European Journal of Education Studies*, *3*, 369–387. https://doi.org/10.5281/zenodo.887089

Alvehus, J. (2013). *Skriva uppsats med kvalitativ metod: En handbok*. Liber.

Amankona, V., Asante, A., Opoku, M., Ohemeng-Gyaase, P., Srekumah, C., Peprah, A. K., & Amankwa-Danquah, P. (2021). Integrating Privacy-By-Design in e-Health. *2021 International Conference on Electrical, Computer and Energy Technologies (ICECET)*, 1–7. https://doi.org/10.1109/ICECET52533.2021.9698489

Arksey, H., & Knight, P. T. (1999). *Interviewing for Social Scientists: An Introductory Resource with Examples*. SAGE Publications.

Bani Issa, W., Al Akour, I., Ibrahim, A., Almarzouqi, A., Abbas, S., Hisham, F., & Griffiths, J. (2020). Privacy, confidentiality, security and patient safety concerns about electronic health records. *International Nursing Review*, *67*(2), 218–230. https://doi.org/10.1111/inr.12585

Bärkås, A., Scandurra, I., Rexhepi, H., Blease, C., Cajander, Å., & Hägglund, M. (2021). Patients' Access to Their Psychiatric Notes: Current Policies and Practices in Sweden. *International Journal of Environmental Research and Public Health*, *18*(17), 9140. https://doi.org/10.3390/ijerph18179140

Berndtsson, M., Hansson, J., Olsson, B., & Lundell, B. (2008). *Thesis Projects—A Guide for Students in Computer Science and Information Systems* (2nd ed). Springer.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Brereton, P., Kitchenham, B. A., Budgen, D., Turner, M., & Khalil, M. (2007). Lessons from applying the systematic literature review process within the software engineering domain. *Journal of Systems and Software*, *80*(4), 571–583. https://doi.org/10.1016/j.jss.2006.07.009

Burkow, T. M., Vognild, L. K., Krogstad, T., Borch, N., Østengen, G., Bratvold, A., & Risberg, M. J. (2008). An Easy to Use and Affordable Home-Based Personal eHealth System for Chronic Disease Management Based on Free Open Source Software. *EHealth Beyond the Horizon – Get IT There*, 83–88.

Busetto, L., Wick, W., & Gumbinger, C. (2020). How to use and assess qualitative research methods. *Neurological Research and Practice*, *2*(1), 14. https://doi.org/10.1186/s42466-020-00059-z

Calder, A., Watkins, S. G., & IT Governance Publishing. (2019). *Information Security Risk Management for ISO 27001/ISO 27002* (3rd ed.). ITGP.

Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., & Neville, A. J. (2014). The Use of Triangulation in Qualitative Research. *Oncology Nursing Forum*, *41*(5), 545–547. https://doi.org/10.1188/14.ONF.545-547

Cellier, L., & Ghernaouti, S. (2019). An interdisciplinary approach for security, privacy and trust in the electronic medical record: A pragmatic legal perspective. *2019 IEEE International Conference on E-Health Networking, Application Services (HealthCom)*, 1–6. https://doi.org/10.1109/HealthCom46333.2019.9009588

Chowdhury, A., & Ray, P. (2007). Privacy Management in Consumer e-Health. *2007 9th International Conference on E-Health Networking, Application and Services*, 29–33. https://doi.org/10.1109/HEALTH.2007.381598

Coppolino, L., D'Antonio, S., Romano, L., Sgaglione, L., & Staffa, M. (2017). Addressing Security Issues in the eHeatlh Domain Relying on SIEM Solutions. *2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*, *2*, 510–515. https://doi.org/10.1109/COMPSAC.2017.45

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, 9.

DOME. (2022). https://domeconsortium.org/

Eckerdal Rivano, J. (2016). Qualitative research methods: Interviewing as a way of learning and knowing. *Journal of the European Association for Health Information and Libraries*, *12*(1), 36–39.

Edemacu, K., Park, H. K., Jang, B., & Kim, J. W. (2019). Privacy Provision in Collaborative Ehealth With Attribute-Based Encryption: Survey, Challenges and Future Directions. *IEEE Access*, *7*, 89614–89636. https://doi.org/10.1109/ACCESS.2019.2925390

E-hälsomyndigheten. (2019, May 22). *Om e-hälsa*. https://www.ehalsomyndigheten.se/om-e-halsa/

Els, F., & 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)*, 1–6. https://doi.org/10.1109/ICTAS.2017.7920658

Entzeridou, E., Markopoulou, E., & Mollaki, V. (2018). Public and physician's expectations and ethical concerns about electronic health record: Benefits outweigh risks except for information security. *International Journal of Medical Informatics*, *110*, 98–107. https://doi.org/10.1016/j.ijmedinf.2017.12.004

Erlingsdottir, G., & Sandberg, H. (2019). E-hälsa—Inte bara teknik. In *På tal om e-hälsa* (pp. 15–25). Studentlitteratur AB.

Eugen, P., & Petru, D. (2018). Exploring the New Era of Cybersecurity Governance. *Ovidius University Annals: Economic Sciences Series*, *18*(1), 6.

European Union Agency for Cybersecurity (EU body or agency), Skouloudi, C., Sarri, A., & Liveri, D. (2015). *Security and resilience in eHealth: Security challenges and risks*. Publications Office of the European Union. https://data.europa.eu/doi/10.2824/217830

Fragidis, L. L., & Chatzoglou, P. D. (2017). Development of Nationwide Electronic Health Record (NEHR): An international survey. *Health Policy and Technology*, *6*(2), 124–133. https://doi.org/10.1016/j.hlpt.2017.04.004

Gajanayake, R., Iannella, R., & Sahama, T. (2011). Privacy by information accountability for e-health systems. *2011 6th International Conference on Industrial and Information Systems*, 49–53. https://doi.org/10.1109/ICIINFS.2011.6038039

Graneheim, U. H., & Lundman, B. (2004). Qualitative content analysis in nursing research: Concepts, procedures and measures to achieve trustworthiness. *Nurse Education Today*, *24*(2), 105–112. https://doi.org/10.1016/j.nedt.2003.10.001

Hägglund, M. (2021, May 18). *Maria Hägglund: Nordic countries lead new initiative on patient access to EHRs*. The BMJ. https://blogs.bmj.com/bmj/2021/05/18/maria-hagglund-nordic-countries-lead-new-initiative-on-patient-access-to-ehrs/

Haufe, K., Colomo-Palacios, R., Dzombeta, S., Brandis, K., & Stantchev, V. (2016). *A process framework for information security management*. *4*(4), 27–47.

Heale, R., & Forbes, D. (2013). Understanding triangulation in research. *Evidence-Based Nursing*, *16*(4), 98. https://doi.org/10.1136/eb-2013-101494

Huckvale, C., Car, J., Akiyama, M., Jaafar, S., Khoja, T., Bin Khalid, A., Sheikh, A., & Majeed, A. (2010). Information technology for patient safety. *Quality and Safety in Health Care*, *19*(Suppl 2), 25–33. https://doi.org/10.1136/qshc.2009.038497

Isaksson, J., & Sanne, T. (2006). *Smarta Kort En del av en intelligent IT-lösning i hälso- och sjukvården?* [Master Thesis, Högskolan i Jönköping]. http://www.diva-portal.org/smash/get/diva2:4290/FULLTEXT01.pdf

Ishaq, A., Qadeer, B., Shah, M. A., & Bari, N. (2021). A Comparative study on Securing Electronic Health Records (EHR) in Cloud Computing. *2021 26th International Conference on Automation and Computing (ICAC)*, 1–7. https://doi.org/10.23919/ICAC50006.2021.9594178

ISO 27799:2016. (2016, July 9). Svenska Institutet För Standarder, SIS. http://www.sis.se/en/produkter/information-technology-office-machines/applications-of-information-technology/it-applications-in-healthcare-technology/ss-en-iso-277992016/

ISO/IEC 27000:2018. (2018). *Information technology—Security techniques—Information security management systems—Overview and vocabulary*. ISO. https://www-sis-se.libraryproxy.his.se/api/document/get/80001198

ISO/IEC 27000:2018. (2018, July 2). Svenska Institutet För Standarder, SIS. http://www.sis.se/en/produkter/standardization/vocabularies/information-technology-office-machines-/isoiec-270002018/

ISO/IEC 27001:2017. (2017, February 28). Svenska Institutet För Standarder, SIS. http://www.sis.se/en/produkter/standardization/information-sciences-publishing/documents-in-administration-commerce-and-industry/sseniisoiec270012017/

ISO/IEC 27002:2022. (2022, February 15). ISO. https://www-sis-se.library-proxy.his.se/api/document/get/8025294

ISO/IEC 27701:2021. (2021, May 25). ISO. https://www-sis-se.library-proxy.his.se/api/document/get/8025294

Jara, H. R., & Schafir, E. (2014). e-Health: An introduction to the challenges of privacy and security. *2014 IEEE Central America and Panama Convention (CONCAPAN XXXIV)*, 1–5. https://doi.org/10.1109/CONCAPAN.2014.7000407

Jesson, J., Matheson, L., & Lacey, F. M. (2011). *Doing Your Literature Review: Traditional and Systematic Techniques*. SAGE. https://books.google.se/books?hl=sv&lr=&id=LUhdBAAAQBAJ&oi=fnd&pg=PP1&dq=Doing+your+literature+review&ots=lD8lgxEXRl&sig=VY-GLyZUPwN1zwCBekfhOya1OQfE&redir_esc=y#v=onepage&q=Doing%20your%20literature%20review&f=false

Johnson, R. B., & Onwuegbuzie, A. J. (2004). Mixed Methods Research: A Research Paradigm Whose Time Has Come. *Educational Researcher*, *33*(7), 14–26. https://doi.org/10.3102/0013189X033007014

Journalen—Inera. (2022, January 25). https://www.inera.se/tjanster/alla-tjanster-a-o/journalen/

Kallio, H., Pietilä, A.-M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: Developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nursing*, *72*(12), 2954–2965. https://doi.org/10.1111/jan.13031

Kamoona, M. A., & Altamimi, A. M. (2018). Cloud E-health Systems: A Survay on Security Challenges and Solutions. *2018 8th International Conference on Computer Science and Information Technology (CSIT)*, 189–194. https://doi.org/10.1109/CSIT.2018.8486167

Karolinska Institutet. (n.d.). *Swedish Medical Subject Headings*. Retrieved 18 March 2022, from https://mesh.kib.ki.se/

Kitchenham, B. (2004). Procedures for Performing Systematic Reviews. *Keele University*, *33*, 33.

Kuo, R.-Z. (2018). EMRS Adoption: Exploring the effects of information security management awareness and perceived service quality. *Health Policy and Technology*, *7*(4), 365–373. https://doi.org/10.1016/j.hlpt.2018.10.012

Lindgren, B.-M., Lundman, B., & Graneheim, U. H. (2020). Abstraction and interpretation during the qualitative content analysis process. *International Journal of Nursing Studies*, *108*, 103632. https://doi.org/10.1016/j.ijnurstu.2020.103632

Loyd Sealy Library. (2018). *Evaluating Information Sources: What Is A Peer-Reviewed Article?* https://guides.lib.jjay.cuny.edu/c.php?g=288333&p=1922599

Lustgarten, S. D., Garrison, Y. L., Sinnard, M. T., & Flynn, A. W. (2020). Digital privacy in mental healthcare: Current issues and recommendations for technology use. *Current Opinion in Psychology*, *36*, 25–31. https://doi.org/10.1016/j.copsyc.2020.03.012

Marshal, R., Gobinath, K., & Venkateswara Rao, V. (2021). Proactive Measures to Mitigate Cyber Security Challenges in IoT based Smart Healthcare Networks. *2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, 1–4. https://doi.org/10.1109/IEMTRONICS52119.2021.9422615

Mayring, P. (2000). Qualitative Content Analysis. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research*, *1*(2), Article 2. https://doi.org/10.17169/fqs-1.2.1089

Meline, T. (2006). Selecting Studies for Systemic Review: Inclusion and Exclusion Criteria. *Contemporary Issues in Communication Science and Disorders*, *33*(Spring), 21–27. https://doi.org/10.1044/cicsd_33_S_21

Mense, A., Hoheiser-Pförtner, F., Schmid, M., & Wahl, H. (2013). Concepts for a Standard based Cross-organisational Information Security Management System in the Context of a Nationwide EHR. *MEDINFO 2013*, 548–552. https://doi.org/10.3233/978-1-61499-289-9-548

Mohammad, Y., & Stergioulas, L. (2010). Building an information security strategy for EHR: Guidelines for assessing the current situation. *2010 Annual International Conference of the IEEE Engineering in Medicine and Biology*, 3919–3922. https://doi.org/10.1109/IEMBS.2010.5627684

MSB. (2018, February 16). *Metodstöd för systematiskt informationssäkerhetsarbete*. http://www.informationssakerhet.se/metodstodet/

Muendo, D. (2014). Information Security Subcultures in Information Security Management: A Conceptual Framework. *European Journal of Business and Management*, *6*(38), 1–8.

Ngozwana, N. (2018). Ethical Dilemmas in Qualitative Research Methodology: Researcher's Reflections. *International Journal of Educational Methodology*, *4*, 19–28. https://doi.org/10.12973/ijem.4.1.19

Nguyen, T. N. M., Whitehead, L., Dermody, G., & Saunders, R. (2022). The use of theory in qualitative research: Challenges, development of a framework and exemplar. *Journal of Advanced Nursing*, *78*(1), e21–e28. https://doi.org/10.1111/jan.15053

NORDeHEALTH. (2022). NORDeHEALTH. https://nordehealth.eu/

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic Analysis: Striving to Meet the Trustworthiness Criteria. *International Journal of Qualitative Methods*, *16*(1), 1609406917733847. https://doi.org/10.1177/1609406917733847

Nurgalieva, L., Cajander, Å., Moll, J., Åhlfeldt, R.-M., Huvila, I., & Marchese, M. (2020). 'I do not share it with others. No, it's for me, it's my care': On sharing of patient accessible electronic health records. *Health Informatics Journal*, *26*(4), 2554–2567. https://doi.org/10.1177/1460458220912559

Oh, S.-R., Seo, Y.-D., Lee, E., & Kim, Y.-G. (2021). A Comprehensive Survey on Security and Privacy for Electronic Health Data. *International Journal of Environmental Research and Public Health*, *18*(18), 9668. https://doi.org/10.3390/ijerph18189668

Okoli, C. (2015). A Guide to Conducting a Standalone Systematic Literature Review. *Communications of the Association for Information Systems*, *37*(1). https://doi.org/10.17705/1CAIS.03743

Özkar, M., & Sandıkkaya, M. T. (2020). A Survey on Security & Privacy Design in e-Health. *2020 5th International Conference on Computer Science and Engineering (UBMK)*, 208–213. https://doi.org/10.1109/UBMK50275.2020.9219372

Patton, M. Q. (2014). *Qualitative Evaluation and Research Methods* (4th ed.). SAGE Publications Inc.

Pocock, T., Smith, M., & Wiles, J. (2021). Recommendations for Virtual Qualitative Health Research During a Pandemic. *Qualitative Health Research*, *31*(13), 2403–2413. https://doi.org/10.1177/10497323211036891

Prasad, B. D. (2019). Qualitative Content Analysis: Why is it Still a Path Less Taken? *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research*, *20*(3), Article 3. https://doi.org/10.17169/fqs-20.3.3392

Priya, R., Sivasankaran, S., Ravisasthiri, P., & Sivachandiran, S. (2017). A survey on security attacks in electronic healthcare systems. *2017 International Conference on Communication and Signal Processing (ICCSP)*, 0691–0694. https://doi.org/10.1109/ICCSP.2017.8286448

Recker, J. (2012). *Scientific Research in Information Systems: A Beginner's Guide*. Springer Science & Business Media.

Reid, R., & Van Niekerk, J. (2014). From information security to cyber security cultures. *2014 Information Security for South Africa*, 1–7. https://doi.org/10.1109/ISSA.2014.6950492

Roig, M. (2006). Ethical writing should be taught. *BMJ : British Medical Journal*, *333*(7568), 596–597. https://doi.org/10.1136/bmj.38946.501215.68

Roller, M. R. (2019). A Quality Approach to Qualitative Content Analysis: Similarities and Differences Compared to Other Qualitative Methods. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research*, *20*(3), Article 3. https://doi.org/10.17169/fqs-20.3.3385

Ronquillo, J. G., Erik Winterholler, J., Cwikla, K., Szymanski, R., & Levy, C. (2018). Health IT, hacking, and cybersecurity: National trends in data breaches of protected health information. *JAMIA Open*, *1*(1), 15–19. https://doi.org/10.1093/jamiaopen/ooy019

Rowe, F. (2014). What literature review is not: Diversity, boundaries and recommendations. *European Journal of Information Systems*, *23*(3), 241–255. https://doi.org/10.1057/ejis.2014.7

Sahama, T., Simpson, L., & Lane, B. (2013). Security and Privacy in eHealth: Is it possible? *2013 IEEE 15th International Conference on E-Health Networking, Applications and Services (Healthcom 2013)*, 249–253. https://doi.org/10.1109/HealthCom.2013.6720676

Sahi, M. A., Abbas, H., Saleem, K., Yang, X., Derhab, A., Orgun, M. A., Iqbal, W., Rashid, I., & Yaseen, A. (2018). Privacy Preservation in e-Healthcare Environments: State of the Art and Future Directions. *IEEE Access*, *6*, 464–478. https://doi.org/10.1109/ACCESS.2017.2767561

Sari, P. K., Handayani, P. W., Hidayanto, A. N., Aji, R. F., & Yazid, S. (2021). Challenges of Inter-organizational Information Security in Healthcare Services: Health Regulator's Perspective. *2021 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS*, 1–6. https://doi.org/10.1109/ICIMCIS53775.2021.9699177

Scandurra, I., Jansson, A., M-L, F.-F., & Alander, T. (2015). Is 'Patient's Online Access to Health Records' a Good Reform? – Opinions from Swedish Healthcare Professionals Differ. *Procedia Computer Science*, *64*, 964–968. https://doi.org/10.1016/j.procs.2015.08.614

Scandurra, I., Pettersson, M., Eklund, B., & Lyttkens, L. (2017). Analysis of the Updated Swedish Regulatory Framework of the Patient Accessible Electronic Health Record in Relation to Usage Experience. *MEDINFO 2017: Precision Healthcare through Informatics*, 798–802. https://doi.org/10.3233/978-1-61499-830-3-798

Schultze, U., & Avital, M. (2011). Designing interviews to generate rich data for information systems research. *Information and Organization*, *21*(1), 1–16. https://doi.org/10.1016/j.infoandorg.2010.11.001

Shen, N., Bernier, T., Sequeira, L., Strauss, J., Silver, M. P., Carter-Langford, A., & Wiljer, D. (2019). Understanding the patient privacy perspective on health information exchange: A systematic review. *International Journal of Medical Informatics*, *125*, 1–12. https://doi.org/10.1016/j.ijmedinf.2019.01.014

Shenton, A. (2004). Strategies for Ensuring Trustworthiness in Qualitative Research Projects. *Education for Information*, *22*, 63–75. https://doi.org/10.3233/EFI-2004-22201

Sjödin, C. (2005, April 13). Dataregister inte bara av godo. Glöm inte patientens integritet! *Läkartidningen*. https://lakartidningen.se/debatt-och-brev/2005/04/dataregister-inte-bara-av-godoglom-inte-patientens-integritet/

The Swedish Patient Data Act (2008:355), no. 2008:355 (2008). https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/patientdatalag-2008355_sfs-2008-355

Ulrichsweb: Global Serials Directory. (n.d.). Retrieved 20 March 2022, from https://ulrichsweb-serialssolutions-com.libraryproxy.his.se/

Vithanwattana, N., Karthick, G., Mapp, G., & George, C. (2021). Exploring a New Security Framework for Future Healthcare Systems. *2021 IEEE Globecom Workshops (GC Wkshps)*, 1–6. https://doi.org/10.1109/GCWkshps52748.2021.9681967

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Wawak, S. (2012). Information Security Management In Context Of Globalization. *Business and Public Administration Studies*, *7*(1), 41–52.

Whitman, M. E., & Mattord, H. J. (2014). *Principles of Information Security, 4th edition* (4th ed.). Cengage Learning. https://www.researchgate.net/publication/311574679_Principles_of_Information_Security_4th_edition

Widmer, T., Premm, M., Schüle, M., Murray, J., & Karänke, P. (2013, June 5). *Distributed knowledge sharing for patient guidance ehealth services*. ECIS 2013 - Proceedings of the 21st European Conference on Information Systems, Utrecht, Netherlands.

Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., Regnell, B., & Wesslén, A. (2012). *Experimentation in Software Engineering [electronic resource]*. Springer Berlin Heidelberg.

Zegers, C. M. L., Witteveen, A., Schulte, M. H. J., Henrich, J. F., Vermeij, A., Klever, B., & Dekker, A. (2021). Mind Your Data: Privacy and Legal Matters in eHealth. *JMIR Formative Research*, *5*(3), e17456. https://doi.org/10.2196/17456

Appendix A - Combination of applied search terms

Database	Search term ID	Search term combination
PubMed	ST1	(("information security" AND ("management system" OR "management systems")) OR ISMS) AND (health* OR care* OR patient* OR health OR care OR healthcare OR patient OR patients) AND (method* OR tool*)) AND pubstatusaheadofprint
	ST2	(("information security" AND ("management system" OR "management systems")) OR ISMS) AND (“digital health” OR “electronic health” OR ehealth* OR "e-health" OR PeHS OR “personal ehealth services” OR “personal e-health services”)) AND pubstatusaheadofprint
	ST3	(("information security" AND ("management system" OR "management systems")) OR ISMS) AND (health* OR care* OR patient* OR ehealth* OR "e-health" OR PeHS OR health OR care OR healthcare OR patient OR patients) AND (secur* OR secure OR security OR privac* OR privacy OR ((data OR data*) AND (protect OR protection OR protect*))) AND pubstatusaheadofprint
	ST4	((electronic* OR computer* OR digit*) AND ((medic* OR health*) AND record*)) AND (secur* OR priva*)
	ST5	((electronic* OR computer* OR digit*) AND ((medic* OR health*) AND record*)) AND (secur* OR priva*) AND (method* OR tool*)
	ST6	(((electronic* OR computer* OR digit*) AND ((medic* OR health*) AND record*)) OR ehealth* OR "e-health" OR PeHS) AND ((individual* OR patient* OR citizen* OR inhabitant*) AND (secur* OR priva* OR sensitiv*))
Medline (EBSCO)	ST1	(("information security" N2 ("management system" OR "management systems")) OR ISMS) AND (health* OR care* OR patient*) AND (method* OR tool*)
	ST2	(("information security" N2 ("management system" OR "management systems")) OR ISMS) AND (“digital health” "electronic health" OR ehealth* OR PeHS OR "personal ehealth services" OR "personal e-health services")
	ST3	(("information security" N2 ("management system" OR "management systems")) OR ISMS) AND (health* OR care* OR patient* OR ehealth* OR "e-health" OR PeHS) AND (secur* OR privac* OR (data* N2 protect*))
	ST4	((electronic* OR computer* OR digit*) AND ((medic* OR health*) N3 record*)) AND (secur* OR priva*)
	ST5	((electronic* OR computer* OR digit*) AND ((medic* OR health*) N3 record*)) AND (secur* OR priva*) AND (method* OR tool*)
	ST6	((electronic* OR computer* OR digit*) AND ((medic* OR health*) N3 record*)) OR ehealth* OR "e-health" OR PeHS) AND ((individual* OR patient* OR citizen* OR inhabitant*) N5 (secur* OR priva* OR sensitiv*))
Scopus	ST1	(("information security" W/2 ("management system" OR "management systems")) OR isms) AND (health* OR care* OR patient*) AND (method* OR tool*))
	ST2	(("information security" W/2 ("management system" OR "management systems")) OR ISMS) AND ("digital health" OR "electronic health" OR ehealth* OR PeHS OR "personal ehealth services" OR "personal e-health services")
	ST3	(("information security" W/2 ("management system" OR "management systems")) OR ISMS) AND (health* OR care* OR patient* OR ehealth* OR "e-health" OR PeHS) AND (secur* OR privac* OR (data* W/2 protect*))
	ST4	((electronic* OR computer* OR digit*) AND ((medic* OR health*) W/3 record*)) AND (secur* OR priva*)
	ST5	((electronic* OR computer* OR digit*) AND ((medic* OR health*) W/3 record*)) AND (secur* OR priva*) AND (method* OR tool*)
	ST6	(((electronic* OR computer* OR digit*) AND ((medic* OR health*) W/3 record*)) OR ehealth* OR "e-health" OR PeHS) AND ((individual* OR patient* OR citizen* OR inhabitant*) W/5 (secur* OR priva* OR sensitiv*))

Appendix B - Bibliography of Accepted Publications

ID	Author	Title	Type
P01	Ishaq et al. (2021)	A Comparative study on Securing Electronic Health Records (EHR) in Cloud Computing	Conference paper
P02	Oh et al. (2021)	A Comprehensive Survey on Security and Privacy for Electronic Health Data	Journal publication
P03	Priya et al. (2017)	A survey on security attacks in electronic healthcare systems	Conference paper
P04	Özkar & Sandıkkaya (2020)	A survey on security & privacy design in e-health	Journal publication
P05	Cellier & Ghernaouti (2019)	An interdisciplinary approach for security, privacy, and trust in the electronic medical record : A pragmatic legal perspective	Conference paper
P06	Kamoona & Altamimi (2018)	Cloud E-health Systems: A Survay on Security Challenges and Solutions	Conference paper
P07	Fragidis & Chatzoglou (2017)	Development of Nationwide Electronic Health Record (NEHR): An international survey	Journal publication
P08	Lustgarten et al. (2020)	Digital privacy in mental healthcare: current issues and recommendations for technology use	Journal publication
P09	Al-Issa et al. (2019)	eHealth Cloud Security Challenges: A Survey	Journal publication
P10	Kuo (2018)	EMRS Adoption: Exploring the effects of information security management awareness and perceived service quality	Journal publication
P11	Ronquillo et al. (2018)	Health IT, hacking, and cybersecurity: National trends in data breaches of protected health information	Journal publication
P12	Nurgalieva et al. (2020)	I do not share it with others. No, it's for me, it's my care: On sharing of patient accessible electronic health records	Journal publication
P13	Els & Cilliers (2017)	Improving the information security of personal electronic health records to protect a patient's health information	Conference paper
P14	Zegers et al. (2021)	Mind Your Data: Privacy and Legal Matters in eHealth	Journal publication
P15	Sahi et al. (2018)	Privacy Preservation in e-Healthcare Environments: State of the Art and Future Directions	Journal publication
P16	Edemacu et al. (2019)	Privacy Provision in Collaborative Ehealth with Attribute-Based Encryption: Survey, Challenges and Future Directions	Journal publication
P17	Bani Issa et al. (2020)	Privacy, confidentiality, security, and patient safety concerns about electronic health records	Journal publication
P18	Coppolino et al. (2017)	Addressing security issues in the eheatlh domain relying on siem solutions	Conference paper

Appendix C - Interview Guide

Intervjuguide

Forskningsintervju relaterat till informationssäkerhet och dataskydd

Öppningsfrågor

- Är det okej om jag spelar in intervjun?
- Jag kommer uppge din roll i masteruppsatsen som kommer publiceras av Högskolan i Skövde. Är det okej att jag också uppger din organisatoriska tillhörighet?

Beskriv masteruppsatsen och syftet med intervjun

Alla frågor fokuserar på utmaningarna med ledningssystem för informationssäkerhet och dataskydd relaterade till invånartjänster som exempelvis 'Journalen'. Jag kommer att presentera en PowerPoint för att göra det lättare att följa med i frågorna.

- Vad har du för roll inom region X?
- Hur ser du på invånartjänster?
    - Vad är dessa tjänsters koppling till ditt arbete?

Frågor relaterade till processen för ledningssystem för informationssäkerhet

Generellt

Hur långt anser du att ni har kommit i ert systematiska arbete med informationssäkerhet/dataskydd?

- Vilka steg i det systematiska informationssäkerhetsarbetet har varit mest utmanande (Plan-Do-Check-Act)?
- Vad hade underlättat processen för att uppnå ett systematiskt informationssäkerhetsarbete?
    - Uppföljning

Invånartjänster

På vilket sätt inkluderar ert systematiska informationssäkerhetsarbete även invånartjänster, som typ Journalen/1177?

- Hur ser processen ut rörande informationssäkerhetsarbetet om nya invånartjänster ska läggas till?
- Vad är de största utmaningarna för invånartjänster i relation till ert informationssäkerhetsarbete/dataskydd?
    - Uppföljning

Verktyg

Vilka metoder och verktyg används i ert systematiska arbete generellt? (ex. MSBs metodstöd, standarder, Klassa, Stratsys)

- På vilket sätt är de tillräckliga?
- Vad kan behöva förbättras?

Täcker era metoder och verktyg upp även kraven på informationssäkerhet och dataskydd gällande invånartjänster, typ Journalen, eller vad krävs ytterligare?

- Uppföljning

GDPR

- Hur påverkade införandet av GDPR det systematiska informationssäkerhetsarbetet?

Frågor relaterade till ansvar

Vem har ansvaret enligt din uppfattning, för att informationssäkerhet/dataskydd hanteras på ett tillfredsställande sätt gällande invånartjänster?

- Uppföljning

Frågor relaterade till användarna

Kunskap

Vilka är utmaningarna kring användarnas (ex. läkare, sjuksköterskor, invånare) kunskap om informationssäkerhet/dataskydd i relation till användningen av invånartjänster (ex. att tjänsterna är finns, vilken information som är tillgänglig)?

- Vad är er upplevelse av utmaningar kring samtycke i relation till invånartjänster?
    - När behövs det och när är det snarare rimligt att inte begära samtycke? (akutsituationer etc.)
        - Uppföljning

Beteende

Vad är utmaningarna med användarnas beteende i relation till användningen av invånartjänster för upprätthållandet av informationssäkerhet/dataskydd?

- Hur kan dessa utmaningar bemötas?
    - Uppföljning

Frågor relaterade till tillgång/behörighet

Behörighetsbehov

Hur hanteras konflikter mellan behörighetsbehov (ex. akuta situationer) och att upprätthålla dataskyddet?

- Är det en konflikt? Varför/varför inte?

Behörighetsansvar

Vem ansvarar för att behörigheterna är lämpliga?

- Uppföljning

Vem ansvarar för att kontrollera att behörigheterna hanteras korrekt?

- Uppföljning

Frågor relaterade till standarder

ISO27000-serien
Underlättar eller försvårar dessa standarder ert systematiska informationssäkerhetsarbete?

- Vad behöver bli bättre?

ISO 27799
Underlättar eller försvårar denna standard ert systematiska informationssäkerhetsarbete?

- Vad behöver bli bättre?

ISO 27701
Underlättar eller försvårar denna standard ert systematiska informationssäkerhetsarbete?

- Vad behöver bli bättre?

Frågor relaterade till applikationer

Vilka utmaningar ser ni med ert systematiska informationssäkerhetsarbete med ökningen av mobila enheter (t.ex. mobiler, smartklockor)?

- Uppföljning

Hur påverkar dessa mobila enheter hanteringen av dataskydd?

- Uppföljning

Frågor relaterade till hot

Vilka är de främsta hoten med invånartjänster?
Hur påverkar det ert systematiska informationssäkerhetsarbete/dataskydd?

- Uppföljning

Frågor relaterade till framtiden

Hur ser ni på framtiden och kommande invånartjänster?

- Hur kompletteras det systematiska informationssäkerhetsarbetet för att inkludera nya tjänster?
- Hur kommer nya tekniker (ex. molnlösningar) påverka det systematiska informationssäkerhetsarbetet/dataskyddet?

Avslutningsfrågor

Är det något mer du vill tillägga som rör utmaningar gällande ledningssystem för informationssäkerhet eller dataskydd som relaterar till användningen av invånartjänster?

- Uppföljning

Appendix D - Interview 1

Interview 1 (I01)
Interviewer: Emelie Mannebäck (E.M)
Respondent: R01 (Funktionsledare informationssäkerhet) and R02 (CISO)

Row	Person	Question and answer	Code
1	E.M	Jag skulle också vilja veta hur ser ni på invånartjänster? Och ser ni någon koppling mellan dessa och vad ni gör i era roller?	
2	R01	Jag tänker att när vi pratar om invånartjänster så är ju, jag skulle vilja vända på frågan lite diplomatiskt och säga när du nämner invånartjänster vad menar du då? Kan du utveckla det lite granna.	
3	E.M	Journalen är ju ett exempel på invånartjänst där du kommer åt exempelvis din elektroniska journal, du kommer åt provsvar, du kan ha direktkontakt med olika vårdinstanser inom vårdkedjan.	
4	R01	Det är bra. Då har vi en likartad bild av vad vi menar med invånartjänster. Och ställer du frågan hur ser vi på invånartjänster som jobbar i en region med ett väldigt tungt hälso- och sjukvårdsuppdrag så är det klart att den typen av tjänster är väldigt centrala för att vi ska kunna fullgöra vårt uppdrag inom regionen. Och det gör ju att förutom de övriga uppdragen vi har inom regionen så precis med alla våra övriga tjänster så behöver vi tänka på informationssäkerhet. Särskilt när det kommer till typ av tjänster som hanterar patientinformation. Det är väl det korta svaret. Så hur vi inom informationssäkerhet i regionen ser på invånartjänster är det en otroligt viktig del av vår verksamhet och det är en otroligt viktig del att vi jobbar med att få så kvalitativa tjänster som vi bara kan för att uppnå det uppdrag vi har att kunna vara där för patienterna. För yttersta så gör vi ju det vi gör inom regionen för att våra patienter bland annat ska ha det så bra som möjligt. Så kan man säga. Vill du komplettera R02?	C04
5	R02	Nej, det lät bra.	
6	E.M	Gött. Då hoppar vi in på det första området som jag kommer ställa några frågor kring. Dessa frågor relaterar till processen för ledningssystem för informationssäkerhet. Inledningsvis på en generell nivå. Så till att börja med, hur långt anser ni att ni har kommit i ert systematiska arbete med informationssäkerhet/dataskydd?	
7	R01	Jag ser inte dig R02. Så du får flika in, men jag kan börja svara inledningsvis. Hur långt vi har kommit vi ansett att vi kommit i det systematiska arbetet utgår från det vi prata om innan, våran roll. Asså våran roll, det vi företräder, det är ju att skapa förutsättningar för ett ledningssystem och jag tycker vi har förutsättningarna för ett systematiskt arbete i regionen. Vi är, man skulle kunna säga en gigantisk organisation, vi har 56 000 anställda och vi är 49 myndigheter inom en och samma organisation. Det gör att det finns utmaningar med att ha ett ensat systematiskt arbete, men jag skulle ändå vilja påstå att vi har ett ledningssystem idag, vi har grundläggande processer och grundläggande organisation till stor del som jobbar utifrån ett systematiskt arbete. Och det har vi haft sen ett par år tillbaka. Så utifrån de förutsättningarna så har vi inom vr organisation skulle jag vilja påstå kommit långt i att sätta de basala och den grundläggande bottenplattan. Sen kan vi alltid jobba med att bli bättre. Vi kan alltid jobba med att tydliggöra våra processer, tydliggöra vår organisation och skapa mer stöttning och stödjande material till den verksamhet som faktiskt utför och jobbar i det dagliga. Där ser vi ju att vi har fortsatt ett kontinuerligt och systematiskt arbete att jobba med, men vi har satt bottenplattan och det är vi väldigt glada för. Vill du komplettera R02?	C04
8	R02	Nej, jag tänker att det är som du sa. Sen som sagt finns det precis som R01 är inne på, det finns liksom saker att göra i flera delar här. Och med tanke på farten på digitaliseringen så kommer det alltid vara så att vi ligger bra till där också skulle jag säga och det finns en bottenplatta och sådär, men vi ja, det finns ett långt arbete liksom kvar att göra för att. I fas vet jag inte om man kommer känna att man är, men det tror jag inte får vara målsättningen heller för det händer så mycket inom det här.	C06
9	E.M	Ni har ju redan varit inne och nosat på det lite, men vilka steg i det systematiska informationssäkerhetsarbetet har varit mest utmanande?	

Row	Person	Question and answer	Code
10	R01	Asså jag skulle säga som R02 är inne på, så är det ju en utmaning att hinna ikapp utvecklingen som sker. Framförallt när vi pratar om kopplat till patientnära tjänster och den typ av digitalisering som en patientnära vård kräver och att patienten är i fokus osv. Där sker ju utvecklingen i enormt rasande kraft. Och det är precis som R02 säger, där behöver vi ha ett tankesätt där vi inte tror att vi kan springa ikapp utan vi måste tänka smartare och mer effektivt och klockar i det vi faktiskt kan göra. Så utmaningen är att hinna med och kunna ligga i framkant, ligga före. Och som sagt om det är möjligt överhuvudtaget, det är väl något jag tror vi mer och mer landar i, att hitta ett annat sätta att försöka fånga in det som måste fångas in i den utveckling som sker.	C04
11	R02	Jag tänker även lagstiftningsmässigt så ser vi ju också att den kommer ju vad ska man säga, lite i efterhand. Ofta liksom här. Vilket gör att då har vi utvecklat saker och ting utifrån rådande lagstiftning, vi behöver liksom backa och lägga raster. Och det behöver vi ju alltid i alla verksamheter, men här är det ju liksom involverade redan väldigt många tekniska komponenter och annat också där det behöver appliceras. Plus då den nya. Så att det är hela tiden den här balansgången liksom. Att ta hand om en ryggsäck och samtidigt liksom hinna ta hand om på förkant. Så precis som R01 säger jag instämmer, där ligger jätteutmaningen.	C04
12	E.M	Vad hade underlättat processen för att uppnå ett systematiskt informationssäkerhetsarbete?	
13	R01	Asså det som hade underlättat det är ju att vi hade haft. Vi hänvisar till varandra R02, men det är ju precis så det är. Hade vi haft en lagstiftning det hade hjälp oss i att skapa goda förutsättningar för ett systematiskt informationssäkerhetsarbete. Det hade ju varit guld värt. Önskvärt. Men när vi dessutom måste tolka lagstiftningen i förhållande till den digitala utvecklingen som sker så blir det knöligt och knepigt. Så all stöttning och vägledning för hur man inom utifrån ett nationellt tänk tänker hade ju underlättat eftersom vi är många aktörer inom samma situationer. Vi får göra väldigt mycket på egen hand. Att få en stöttning i dem och en riktning i hur Sverige och nationellt tänker hade varit önskvärt.	C01, C02
14	E.M	Och den här tolkningen som du pratar om. Har ni upptäckt att man gör det för sig själv i varje region eller samarbetar man mellan regioner för att försöka hitta gemensamma nämnare så att man åtminstone lägger sig åt samma spår? Eller får alla klara sig på egen hand?	
15	R01	Det sker ju ett regionalt samarbete i vissa delar, men ytterst och till synes och sist så är vi ju enskilda myndigheter med ansvar för vår egen information. Och riskägarskapet kan vi aldrig liksom överlåta till någon annan, utan här handlar om att utifrån den samsyn som man kan skapa nationellt så behöver var och en gå hem till sig och fundera över vilka risker vi är villiga att ta utifrån de förutsättningar som vi har i vår organisation. Naturligtvis, all dialog och som sagt samarbete man kan skapa är ju till gagn för att kanske landa i de egna värderingarna och bedömningarna man gör inom sin organisation. Men till synes och sist har vi ett eget ansvar för den information som regionen hanterar och som respektive myndighet inom regionen hanterar. Det måste vi komma ihåg även om vi har samverkan organisationsgränser emellan.	C03
16	E.M	Vidare, på vilket sätt inkluderar ert systematiska informationssäkerhetsarbete även invånartjänster, som typ Journalen/1177?	
17	R01	Det var som jag sa inledningsvis. Utifrån den storlek på organisation som vi är så har vi ju ett antal tjänster som vi förvaltar och som vi tillhandahåller. Och det ledningssystem för informationssäkerhet och dataskydd vi har det ska tillämpas och är tillämpbart på samtliga våra tjänster. På samma sätt som vilken annan tjänst som helst skulle jag säga att det korta svaret är att det ska vara ett systematiskt informationssäkerhetsarbete även för invånartjänsterna. På samma sätt som vilken annan tjänst som helst då.	C06
18	E.M	Då blir det säkert lite upprepning här. Hur ser processen ut rörande informationssäkerhetsarbetet om nya invånartjänster ska läggas till?	
19	R01	Det är precis som du säger. Även där. Samma struktur gäller för nya invånartjänster som för andra system. Att det finns en införandeprocess som är kvalitativ och säkerställer att de perspektiv och de analyser som behöver göras inför ett införande att det sker enligt konstens alla regler utifrån det som vårt ledningssystem pekar på.	C06
20	E.M	Vad är de största utmaningarna för invånartjänster i relation till ert informationssäkerhetsarbete/dataskydd?	

Row	Person	Question and answer	Code
21	R01	Här tror jag att vi egentligen hade behövt fråga dem som jobbar närmare det dagliga kopplat till invånartjänsterna. Med det är klart om man tittar generellt sätt på vilka utmaningar har vi med ett systematiskt informationssäkerhetsarbete så är det ju att integrera informationssäkerhetsarbetet så tydligt som det behöver vara i tjänster som det finns en väldigt stor verksamhetsnytta kring. Alltså, om vi backar tillbaka till det vi pratade om förut. Vi behöver jobba systematiskt med vår information och säkerhetsarbetet kopplat till det. Och det innebär att vi behöver göra ganska knepiga analyser ibland och framförallt när det kommer till tjänster som har en väldigt stor verksamhetsnytta så är det viktigt att balansen är väldigt tydlig, att man får med samtliga perspektiv och att processerna säkerställer att vi får med informationssäkerhetsarbetet och perspektivet informationssäkerhet/dataskydd när vi för in och när vi förvaltar. Det gäller ju gäller ju generellt sätt för alla tunga tjänster som så att säga har en väldigt stor vikt för att uppnå en patientnytta eller en verksamhetsnytta, så blir det ännu viktigare att få en balans skulle jag säga. Jag vet inte R02 om du vill komplettera något där?	C04
22	R02	Nej, jag tänker att jag inte behöver det.	
23	E.M	Då går vi vidare. Det finns flertalet olika metoder och verktyg för att designa och hantera ledningssystem för informationssäkerhet exempelvis MSBs metodstöd, standarder, Klassa, Stratsys. Vilka metoder och verktyg används i ert systematiska arbete generellt?	
24	R01	Alltså vårt ledningssystem bottnar sig i ISO standarder 27000-serien primärt och även MSBs metodstöd är ju en viktig grundplatta för hur vi byggt vårt ledningssystem och de verktyg, metoder och modeller som vi använder. Sen har vi ju också. Det finns just precis du säger, det finns andra standarder och framförallt inom cybersäkerhet och IT-säkerhet. Där finns det ju andra standarder och kompletterande ramverk som är kompatibla med ISO standarderna och 27000-serien, som också tillämpas. Men det vi jobbar för är att de standarder och ramverk vi använder i organisationen, att det ska vara kompatibelt så att säga. De ska inte motverka eller så, utan de ska kunna vara kompatibla i de analyser som vi faktiskt gör. Med det bero liksom lite på eftersom vi har så otroligt många verksamheter och där det är olika standarder som träffar de olika verksamheterna och informationen inom ramen för det så är det ändå ISO standarderna som är paraplyet kan man säga.	C06
25	E.M	Och på vilket sätt är dessa metoder och verktyg ni använder tillräckliga?	
26	R01	Ja, det är en liten lurig fråga för man skulle ju kunna tänka sig att frågan är ställd utifrån 'uppnår vi då det säkerhetsarbetet som vi vill uppnå med de metoderna' och det är ju något som vi var inne på förut. Vi kan alltid bli bättre, men de metoder och verktyg vi har utifrån det jag sa om att vi har en plattform att utgå från i vårt systematiska arbete så har vi verktyg, metoder och modeller för att kunna ha förutsättningar att jobba på ett säkert sätt med den information som vi hanterar. Sen behöver vi skruva i de metoderna och verktygen också för att hänga med och för att ja av olika skäl liksom bli ännu bättre i dem strukturer och metoder vi har. Men vi har verktygen för att kunna verka på det sätt som vi vill verka, så kan man säga.	C06
27	E.M	Du är som tidigare inne och nosar redan på min nästa fråga. Vad kan behöva förbättras i dessa metoder och verktyg för att underlätta i arbetet?	
28	R01	Det är ju ett hantverk. Det kräver handpåläggning. Det kräver tid. Det kräver kompetenshöjning. Det kräver att vi lär av varandra och att vi lär av de erfarenheterna för att bli ännu bättre. Så jag tänker att det som vi inom, tittar än en gång på vårt uppdrag, ifrån vår enhets sida så är det ju att kunna stötta verksamheterna i metoderna och kunna vara tydligt informera, kommunicera om vilka metoder och verktyg som vi har så att det inte glöms bort. Så att vi kan erfarenhetshantering, så att vi kan ge bra exempel på hur man kan göra. Allt för att höja kompetensen hos de som faktiskt jobbar med analyserna. Och det tror jag är jätteviktigt. Det här återkommande och då är vi inne i det systemiska, att fortsätta orka hålla i och prata om de här frågorna och att också förstå varför har vi de här metoderna. Varför vill vi att ni ska analysera, jo för att det faktiskt gagnar er som ansvarar för informationen. Att det blir ett så lämpligt skydd för information som bara möjligt och då har ni hjälp av de här metoderna och verktygen för att kunna uppnå det.	C06, C07
29	E.M	Täcker era metoder och verktyg upp även kraven på informationssäkerhet och dataskydd gällande invånartjänster, typ Journalen, eller krävs det något ytterligare för att kunna arbeta där?	
30	R01	Nä men metoderna och verktygen är ju generiska och generella så de ska ju vara applicerbara oavsett tjänst, oavsett typ av information kan man säga. Däremot så är det ju	C06

Row	Person	Question and answer	Code
		viktigt att vi har ett nära samarbete med våra systemförvaltare och informationsägare. Och att vi kan fånga upp behov av förändring av de metoder och verktyg som vi har, just för att kunna hitta vad vi behöver skruva utifrån vad den här typen av information, verksamhet och tjänst är i behov av. Så det är ju ett samspel mellan vår informationsägare och systemägare att vi ska tillhandahålla de bästa verktyg vi kan för att det ska bli så bra som möjligt i slutändan.	
31	E.M	Till sist, hur påverkade införandet av GDPR det systematiska informationssäkerhetsarbetet?	
32	R01	Man kan ju säga, och du vill säkert säga något här R02, men man kan ju säga att GDPR var ju en, det gjorde att man kraftsamlade sig för införandet och att fokuset blev på det här området och informationssäkerhetsarbetet i stort. Vilket är ju väldigt positivt tycker jag och vi som jobbar med informationssäkerhet. Det kommer upp på agendan. Så där riktades ju ögonen mot dem processer vi har inom informationssäkerhet och det var ju positivt R02.	C05
33	R02	Ja, det var det. Det satt ju lupp på dem delarna i arbetet och det har vi kunnat bygga vidare på och det som kom fram där. Som sagt det gjorde verkligen att organisationen intensivt arbetade med de här frågorna och fick då upp de på bordet och ökade kompetens och kunskapsnivån inom det också.	C05
34	E.M	Härnäst undrar jag hur ansvar hanterats i relation till invånartjänster. Vem har ansvaret enligt er uppfattning, för att informationssäkerhet/dataskydd hanteras på ett tillfredsställande sätt gällande invånartjänster?	
35	R01	Där har vi ju en organisationsmodell och en förvaltningsmodell som, informationsägarskapet följer alltid linjen så att säga. Den som hanterar information däri finns också ett informationsägarskap. Men vi har ju en organisationsmodell framförallt skulle jag säga till följd av den storlek vi är, att vi har en regional förvaltningsmodell där tjänster hanteras och förvaltas på regional nivå. Och det gör ju att de som ansvarar för införandet av ett system eller förvaltning av system har också ett visst ansvar för att säkerhetsställa att systemet uppfyller det som den ska och att den har det skydd som verksamhetsinformationen kräver. Så informationsägarskapet ligger kvar men man har på något sätt företrädarskap att säkerhetsställa skyddet för informationen är på det som verksamheten behöver ha. Då ligger det inom ramen för det vi kallar pm3 modellen då hos oss, en IS/IT styrmodell som bygger på en regional hantering och regional förvaltning med en verksamhets sida och en IT-sida.	C06
36	E.M	Nästa område relaterar till användarna som i den här studien inkluderar samtliga typer, exempelvis läkare, sjuksköterskor och invånare i sig. Vilka är utmaningarna kring användarnas kunskap om informationssäkerhet/dataskydd i relation till användningen av invånartjänster? Exempelvis att tjänsterna ens finns, vilken information som är tillgänglig osv.	
37	R01	Här känner jag ju att jag har egentligen lite svårt att kommentera. Det här är ju något som är mer nära invånartjänsterna. Jag tror att under hela det här avsnittet kopplat till användarna skulle jag nästan vilja, inte passa på frågan för det är fel, men det blir nästan en gissningslek utan förankring med de som jobbar med invånartjänsterna. Så vad säger du om att vi inte går in i dem svaren?	
38	E.M	Om ni inte känner er bekväma med att svara så är det helt okej. Då gör jag gärna en uppföljning via mejl istället.	
39	R01	Absolut, så kan vi göra. För då hinner jag stämma av med de som jobbar med och förvaltar våra invånartjänster, för att få deras uppfattning kring det så kan vi tillsammans återkomma med ett svar till dig. För det är som sagt mycket kopplat till hur de upplever det tror jag. Både som du säger våra egna användare men också patienterna. Så det är dumt att vi gissar tänker jag.	
40	E.M	Då kommer jag bara visa de nästkommande två frågorna på området så att ni har sett dem. Nästa fråga är då vad är er upplevelse av utmaningar kring samtycke i relation till invånartjänster? För inspelningens skull kan ni säga pass.	
41	R01	Jag säger pass då.	
42	E.M	Nästa fråga hade då blivit, när behövs det och när är det snarare rimligt att inte begära samtycke? Exempelvis vid akutsituationer.	

Row	Person	Question and answer	Code
43	R01	Jag säger pass där också.	
44	E.M	Nästa fråga fortfarande relaterat till användarna handlar om beteende. Vad är utmaningarna med användarnas beteende i relation till användningen av invånartjänster för upprätthållandet av informationssäkerhet/dataskydd?	
45	R01	Jag säger pass där också.	
46	E.M	Hur kan dessa utmaningar bemötas?	
47	R01	Jag säger pass där också.	
48	E.M	Nästkommande frågor berör tillgång och behörighet. Hur hanteras konflikter mellan behörighetsbehov exempelvis akuta situationer och upprätthållandet av dataskyddet i relation till invånartjänster?	
49	R01	Då är vi inne på det som vi snuddade lite på förut. Vi har olika typer av regelverk att förhålla oss till i grunden. Och ibland så är det ju inte heller att lagstiftningarna pekar mot samma riktning, de kan till och med stå direkt emot varandra, och därtill så har vi vårt uppdrag att skapa de bästa förutsättningarna och ge den bästa vården till patienten. Det är inte heller alltid den nyttan som överensstämmer med vad lagstiftningen pekar på eller där lagstiftningen går stick i stäv med varandra. Då är ju utmaningen och det som vi som organisation måste göra är att förhålla till samtliga av dessa aspekterna och göra en avvägning. En kvalitativ sådan utifrån riskanalyser, klassning av information osv för att kunna skapa oss en total bild av vad vi har att förhålla oss till. Det är ju klart att då är det avvägningar som måste göras, men det är otroligt viktigt än en gång, då är vi tillbaka till riskägarskapet, att man vet vilka risker man har att förhålla sig till och hur man kan mitigera och minimera dem i största möjligaste mån. Och som sagt om det är lagstiftning som då går i stick och stäv med varandra så ytterst är det en avvägning i det enskilda fallet det som är till förmån till det man vill uppnå eller hur man når det man vill uppnå på något sätt. Men den kvalitativa beredningen, de kvalitativa analyserna är ju grunden för att kunna fatta kloka och väl avvägda beslut. Det är ju det som vi jobbar hårt för att kunna skapa de strukturerna för så att när vi måste göra eventuella avvägningar så gör vi det på ett klokt sätt	C01, C06
50	E.M	Nästa fråga är, som jag också känner att du redan besvarat. Är det en konflikt? Som du säger, lagstiftning. Är det andra aspekter som påverkar den här konflikten?	
51	R01	Det kan ju finnas olika perspektiv framförallt. Jag tänker att det inte alltid nödvändigtvis, det är lagstiftning i botten men det kan finnas olika perspektiv för stunden som väger mer eller mindre tungt kan man säga. Och alla dessa olika perspektiv måste in i samma kastrull och röras om och liksom verkligen ångas av om jag uttrycker mig med den liknelsen för att man ska kunna vrida och vända på det på absolut bästa sätt. Så är det. Det är många, det är sällan ett perspektiv, en lagstiftning att förhålla oss till utan det är mer komplext än så ska jag säga.	C04
52	E.M	Gällande behörighetsansvar. Vem ansvarar för att behörigheterna är lämpliga i relation till invånartjänster?	
53	R01	Ja, om jag inte ska dra en lång föreläsning om våra styrande dokument gällande behörighet och åtkomst, men i korthet och generellt sätt ska kan vi väl säga att den som ansvarar för informationen är ju också den som ansvarar för att rätt person har åtkomst till rätt information. Och oftast kanske det ligger ett eller oftast är det ju en chef som vet vilka behörighet ska dess medarbetare ha för en åtkomst till en tjänst och en information så att säga om vi pratar i generella termer. Men det utgår från informationsägarskapet så att rätt person har rätt behörighet till rätt information då och i rätt tid som också är otroligt viktigt. Och här har vi då en regional modell, regionala styrande dokument för hur behörighetstilldelning ska gå till och vi har också då utifrån den förvaltningsmodell som vi har så är det upp till systemägare och systemförvaltare att säkerställa att tjänsterna är kompatibla med den typen av behörighetshantering som vi inom regionen har valt att ha. Eller valt att ta, har att förhålla oss till ska jag säga. Så det är en trestegsraket, vi har regionala strukturer, vi har de som regionalt förvaltar och implementerar det som ska finnas kopplat till en tjänst och sen har vi ett informationsägarskap och en verksamhet som bedömer lämpligheten av de behörigheter som våra medarbetare ska ha	C06
54	E.M	Vem ansvarar för att kontrollera att behörigheterna hanteras korrekt i relation till invånartjänster?	

Row	Person	Question and answer	Code
55	R01	Det följer egentligen samma struktur. Det vill säga att om du som chef har medarbetare med behörighet till ett system så har du ett ansvar att säkerställa att de är uppdaterade och att det inte sker några förändringar som gör att man behöver skruva i behörigheterna. På samma sätt de som förvaltar systemet har ett uppföljningsansvar att säkerställa att den behörighetsmodell som systemet tillhandahåller och ska följa att det följs av de som nyttjar systemet. Och ytterst om vi backar ett steg. Vi på ESB som enhet som ansvarar för ledningssystemet för informationssäkerhet har ett ansvar att säkerställa att de som förvaltar systemet också implementerar regionens synsätt på behörighetshantering i de tjänster som förvaltas. Så det följer på samma sätt då.	C06
56	E.M	Härnäst kommer ett par frågor om de standarder som berör informationssäkerhet och dataskydd samt hanteringen av detta inom hälso- och sjukvård. Först och främst, ISO 27000-serien Underlättar eller försvårar dessa standarder ert systematiska informationssäkerhetsarbete? Vad behöver bli bättre?	
57	R01	Jag vet inte R02, vill du ha några inspel kring detta? Min personliga uppfattning och det är verkligen en personlig uppfattning, det är att alla strukturer och standardiseringar vi har underlättar i dialogen vi har med andra. Det vill säga vi vet att när vi pratar ISO 27000-serien så vet vi vad vi pratar om. Vi vet vad vi verkar i när vi pratar om det. Så personligen tycker jag att allt som är en standardiserad grundplattform underlättar och det är också så som vi har valt att tillämpa ISO 27000-serien som ett hjälpmedel. Så jag skulle säga att det underlättar vårt arbete. Sen är ju utmaningen att det finns många standarder som vi var inne på förut, men där är det ju också ett väldigt bra arbete generellt kring att de är kompatibla och de är så pass generella att det går att ha olika typer av ramverk som ändå jobbar tillsammans. Jag upplever personligen inte att det blir konflikter. Hade det blivit det så hade det varit en utmaning, men eftersom de är så breda och det handlar om metoder och ett arbetssätt så underlättar de i det dagliga arbetet. Och framförallt i dialogen med andra som nyttjar samma serier. Vill du komplettera något där R02?	C02
58	R02	Nä, men jag instämmer helt med vad R01 säger. Alltså allt som kan standardiseras är liksom bra för det ger stöd och stöttning. Det som väl apropå vad kan bli bättre, liksom utmaning i det här är ju vi har väldigt många delar här att arbeta med i organisationen om man säger så. Och det här kommer från ett perspektiv och det är ju just att kunna knyta an dem i det ledningssystem som vi ändå valt att arbeta med och i organisationen. Att liksom kunna vara, vad ska man säga, att få dem här standarder och annat att hitta en följsamhet i hur vi behöver liksom hantera och organisera själva helheten för att kunna omhänderta alla dessa olika perspektiven. Så där är väl såna delar som just, jag skulle inte säga att det är något som kan förbättras men det är en sån del som kan tas som en utmaning i det. Annars är risken att det blir väldigt mycket stuprör över det hela, nu jobbar vi med det här spåret och sen tittar vi på en annan fråga eller har ett annat perspektiv och då jobbar vi i det spåret, så att få dem att skäras så. Men i övrigt precis det som R01 säger liksom. Allt som kan standardisera ger vägledning och stöd och stöttning är av godo.	C04, C02
59	E.M	Sen finns också ISO 27799 som är en förlängning av 27000-serien för hälso- och sjukvård. Underlättar eller försvårar denna standard ert systematiska informationssäkerhetsarbete? Vad behöver bli bättre?	
60	R01	Och nu då bara så jag har gjort min hemläxa det är den som är kopplat till informatikdelarna?	
61	E.M	Ja, precis.	
62	R01	Bra. Och här blir det väldigt tydligt. Jag tycker det är jättebra att du lyfter det R02, hur standarderna ska kopplas samman i en helhet och inte jobbas med i stuprör. Jag säger inte att det är så i den här, men det är tydligt exempel på när vi har mer specifika standarder kopplat till vissa områden. Som du säger hälso- och sjukvården är ju en av dem områdena, det är ett tungt område inom vår region naturligtvis men det är specifika standarder som kanske är mer tydliga inom vissa verksamheter än inom andra. Men vi ska ändå ha ett ensat och ett ledningssystem som är tillämpbart i alla led. Och då är det jätteviktigt och vi jobbar nu faktiskt med att tydliggöra de standarder som vi har att förhålla oss till så att vi får den här kartbilden tydligare än vad vi faktiskt har idag utifrån att vi får en ny, det kommer en ny 27002 så ser vi över de standarder som vi har att förhålla oss till och även en ny 27001 för den delen. Så vi gör det här trädet med standarder som vi behöver förhålla oss till lättare för verksamheten att se hur saker och ting hänger ihop. För det är viktigt tror jag. Vi som jobbar med standarder och vet hur de hänger ihop det är ju bra, men det är också så att när man jobbar med ISO 27799 att man som du sa ser att det är en förlängning på något annat och att verksamheten som jobbar utifrån ett ramverk och informatiken inom hälso- och sjukvård kan se helheten	C06

Row	Person	Question and answer	Code
		än en gång. Det är så otroligt viktigt i en stor organisation så att det inte tenderar att bli separata spår. Men än en gång här är det ju asså generellt sätt när det kommer till standarder så allt som kan ge en stöttning eller vägledning är bra.	
63	E.M	Till sist finns ISO 27701 som är en förlängning av ISO 27001 och berör insamling samt hantering av personuppgifter. Och skapades väl först och främst i och med införandet av GDPR just för att förenkla arbetet. Underlättar eller försvårar denna standard ert systematiska informationssäkerhetsarbete? Vad behöver bli bättre?	
64	R01	Det är egentligen samma sak. Samma svar som tidigare. Det underlättar för att det på något sätt ändå tydliggör hur man kan tänka, hur man kan jobba. Och framförallt kopplat till GDPR så upplevde jag att det var till hjälp att det kom standarden som pekade på det arbetet som vi redan gör inom ramen för 27001 och 27002 då behöver man docka in det här utifrån ett GDPR perspektiv, men man skapar inget separat spår, man integrerar det i det redan befintliga arbetet. För det är ju än en gång ett typexempel på att GDPR som så många andra lagstiftningar skapar egna spår och egna processer istället för att integrera dem i redan befintligt arbete. Så att nej, bara bra att det finns ramverk att förhålla sig till.	C05
65	E.M	De följande två frågorna berör de olika typerna av applikationer. Först, vilka utmaningar ser ni med ert systematiska informationssäkerhetsarbete med ökningen av mobila enheter exempelvis som mobiler, smartklockor?	
66	R01	Asså, generellt sätt om man tittar på det u från ett informationssäkerhetsperspektiv så ju fler enheter vi har desto bättre behöver vi va på att säkerställa informationssäkerheten hela vägen ut. Och säkerställa kontrollerna av information alldeles oavsett vilken enhet. Men än en gång, det är liksom så verkligheten ser ut och det är det som vi behöver jobba på för att hinna med i den takt som utvecklingen sker för det är så verkligheten ser ut. Och det är ingen idé att förneka det, utan hitta ett arbetssätt som kan hinna ikapp med den utvecklingen som är. Men som sagt det kräver att man också hela vägen ut i organisationen förstår att ju fler enheter vi har som kan konsumera den information som vi har dessutom mer effektivt behöver vi jobba med informationssäkerhet och dataskydd hela vägen ut i alla enheter. Så kan man säga.	C04
67	E.M	Hur påverkar dessa mobila enheter hanteringen av dataskydd?	
68	R01	Ja, det är ju samma som frågan ovan. Som sagt, dataskyddet än en gång, vi jobbar mycket med att ha en integrerat informationssäkerhet och dataskydd. Vi kalla också vårat ledningssystem för ett ledningssystem för informationssäkerhet och dataskydd ska jag säga. Men på samma sätt här, det flödar otroligt mycket information dagligen och vi behöver jobba för att skruva våra processer och säkerställa att det finns en kompetenshöjning i organisationen kring lättheten i att kunna olika typer av enheter för att konsumera informationen.	C04
69	E.M	Härnäst är jag intresserad av ditt/ert perspektiv på hot kopplade till invånartjänster. Vilka är de främsta hoten med invånartjänster?	
70	R02	Kan du utveckla liter mer med vad du menar med hot? Alltså i vilken kontext.	
71	E.M	Ja, utifrån den kontext som ni vill svara utifrån skulle jag kunna kontra med. Utifrån den litteraturstudie som jag genomfört är fokuset mycket för just invånartjänster hot. Och då är det allt från nätverkshot till konstaterande att attackytan har ökat i och med införandet av applikationer som mobila enheter osv. Men även hot utifrån användares beteende och liknande. Och då är ju frågan utifrån ert perspektiv, vad är främsta hoten som ni ser mot invånartjänster?	
72	R02	Jag vet inte om jag kan svara specifikt för tjänster om man säger just för dem, men rent generellt så kan man väl säga och det är ju det här vanliga att desto mer digitala vi blir desto mer sårbara blir vi också. Både utifrån att de som inte ska få tillgång till information får tillgång till den, utifrån att informationen inte är riktig eller korrekt och när du pratar om flera attackytor och liknande det vet vi ju med oss, med omvärldsläget som vi har nu också. Just att det finns en stor, vad ska jag säga, det finns liksom en riskbild kopplat till den information som vi har sparad digitalt överhuvudtaget. Och här är ju också ett arbete om man ska koppla an där som ju behöver göras överhuvudtaget på våra system eller på vår information ska jag säga och vart vi har den vad gäller säkerhetsskyddet också. Alltså finns det delar här i som också kan ha betydelse för Sveriges säkerhet. Så skulle jag säga, men det är ju inte kopplat rent till invånartjänsterna men det är liksom rent allmänt. Ett sånt resonemang. Men R01 du får fylla på här.	C04

Row	Person	Question and answer	Code
73	R01	Nä men det var alldeles ypperligt tänker jag. För det var därför jag grunnade lite på, för jag kan inte heller ange någon specifik risk kopplat till invånartjänster utan det är precis som R02 säger. Ju fler användare, ju fler konsumenter av information, desto mer information vi har och desto fler ytor vi har desto mer sårbara är vi och då behöver ju jobba ännu mer aktivt och effektivt utifrån det ledningssystem vi har. Så inga mer kompletteringar till det från min sida.	C04
74	E.M	Hur påverkar det ert systematiska informationssäkerhetsarbete/dataskydd utifrån de hot som ni nämnt?	
75	R01	Det är ju grundbulten. Om vi ska kunna möta omvärlden, om vi ska kunna möta verkligheten måste vi förstå de behov som finns, de hot som finns, de aspekterna vi behöver ta hänsyn till för att kunna skruva i vårt systematiska informationssäkerhetsarbete för att det blir så effektivt som möjligt. Alltså gäller det att ligga i framkant i att lyssna av och också våga utveckla om jag uttrycker mig så, för det kan ju också vara en utmaning i en stor organisation men vi måste jobba aktivt med att ha robusta processer och robusta strukturer men som hela tiden utvecklas. Och hitta den balansen för att kunna möta hur verkligheten ser ut. Så vi kan inte luta oss tillbaka är väl egentligen budskapet, utan vi måste finnas med och hela tiden utvecklas.	C04, C07
76	E.M	De sista frågorna berör framtiden. Hur ser ni på framtiden och kommande invånartjänster? Och jag slänger upp följdfrågorna direkt. Hur kompletteras det systematiska informationssäkerhetsarbetet för att inkludera nya tjänster? Hur kommer nya tekniker exempelvis molnlösningar påverka det systematiska informationssäkerhetsarbetet/dataskyddet?	
77	R01	Jag skulle säga att jag vill svara på samma sätt som för föregående fråga. Vi måste, dels måste vi försöka tänka långsiktigt utifrån som du säger den utveckling som sker och där har vi ju experter höll jag på att säga inom andra verksamheter framförallt inom hälso- och sjukvården som ser 'vad behöver vi ha för att kunna möta våra invånares behov och patienters behov'. Det är ju liksom grunden, vad är behovet. Och sen behöver vi ju utifrån det möta och jobba aktivt med att utveckla ledningssystemet så att vi än en gång kan möta de behov som finns. Så det här är ju ett samspel och där vi behöver skapa strukturer där det samspelet kan verka på ett effektivt sätt. Men det är klart att vi behöver än en gång inte luta oss tillbaka utan försöka ligga så mycket i framkant som vi bara kan. Men jag tror som vi sa i början av intervjun att det är svårt att ligga före i den takt som digitaliseringen sker, men att hitta former för att ändå möta det behovet på något sätt då.	C04
78	E.M	Avslutningsvis, är det något mer du/ni vill tillägga som rör utmaningar gällande ledningssystem för informationssäkerhet eller dataskydd som relaterar till användningen av invånartjänster?	
79	R01	Nej, jag tycker du har fångat helheten i dina frågor så jag har inget att lägga till där.	
80	E.M	Finns det andra utmaningar gällande ledningssystem för informationssäkerhet eller dataskydd som du vill lyfta som inte berör invånartjänster?	
81	R01	Nej, jag tycker att du i dina frågor också har fångat dem, hur ska jag säga. Alltså vi pratar ju mycket generellt under intervjun kring det systematiska arbetet som ju är applicerbart i invånartjänster och i andra tjänster. Så vi har nog berört de utmaningar som vi ser och som vi jobbar aktivt med för att kunna bli bättre.	

Appendix E - Email after interview 1

Email from respondent R01:

Nästa område relaterar till användarna som i den här studien inkluderar samtliga typer, exempelvis läkare, sjuksköterskor och invånare i sig. Vilka är utmaningarna kring användarnas kunskap om informationssäkerhet/dataskydd i relation till användningen av invånartjänster? Exempelvis att tjänsterna ens finns, vilken information som är tillgänglig osv.
Det finns en utmaning inom samtliga regioner att nå ut med information till medarbetare i vården om tjänster som används av patienter/invånare. Vår region har bra information till medarbetare men vi kan bli ännu bättre på att ta oss tid att uppdatera oss på vad som gäller och säkerställa att nya medarbetare informeras om gällande rutiner

Nästa fråga är då vad är er upplevelse av utmaningar kring samtycke i relation till invånartjänster?
Vårdpersonal måste alltid fråga om samtycke vid t.ex. uthopp till nationella tjänster och här tycker jag att vår region har fått ut informationen bra och att det är en fungerande rutin. Vi har haft detta igång sedan 2012 och nu efter några år har vi utöver välinformerad personal också välinformerade invånare som kan begränsa tillgång till information när dem så önskar.

Nästa fråga hade då blivit, när behövs det och när är det snarare rimligt att inte begära samtycke? Exempelvis vid akutsituationer
Det går inte att begära samtycke om patienten inte är kontaktbar. Där är det vårdpersonals bedömning om det behövs göras en nödöppning för att få all tillgänglig information för att kunna ge patienten bästa vård och behandling. Här tycker jag att dem rutiner vi har fungerar mycket väl.

Nästa fråga fortfarande relaterat till användarna handlar om beteende. Vad är utmaningarna med användarnas beteende i relation till användningen av invånartjänster för upprätthållandet av informationssäkerhet/dataskydd
Vårdpersonal som dokumenterar i patientjournal ska ha kunskap som vad som blir synligt för invånaren som läser sin journal och ha tillgång till rutiner för att undanta information som inte ska visas. Vi kan också skydda barnen via upprättade rutiner och dessa rutiner fungerar bra men kännedomen om att det också går att ge tillgång till information i journal när ungdom är 13-15 år behöver bli tydligare. Den tillgången kan gälla för ungdom och/eller en eller båda vårdnadshavarna. Om vi ska få ökad användning av våra invånartjänster måste vi få igång bättre information om möjligheter.

Hur kan dessa utmaningar bemötas?
Genom information, utbildning och dialoger. Som region behöver vi vara ”ute” och synas där både invånare och vårdpersonal finns. Vi behöver ha en ”kiosk” för att informera om invånartjänster på t.ex. regionens sjukhus, vi behöver synas hos patientförening med mera.

Appendix F - Interview 2

Interview 2 (I02)
Interviewer: Emelie Mannebäck (E.M)
Respondent: R03 (Cybersäkerhetsspecialist)

Row	Person	Question and answer	Code
1	E.M	Hur ser du på invånartjänster? Och hur är dessa tjänster kopplade till ditt arbete?	
2	R03	Ja, alltså mitt jobb går ju delvis ut på att flambera våra egna lösningar så att vi håller oss on par med lagstiftningen och det där har ju vässats ordentligt efter tjänst 2 domen i EU domstolen. Privacy shield rök. Då har vi alltså system som vi behöver titta närmare på. Kanske lyfta in i huset.	
3	E.M	Gott. Nu kommer ett antal frågor relaterade till processen för ledningssystem för informationssäkerhet. Och börjar vi med ett par generella frågor. Till att börja med, hur långt anser du att ni har kommit i ert systematiska arbete med informationssäkerhet/dataskydd?	
4	R03	Jag tycker att vi har kommit riktigt långt och vi vinner nya framgångar varje dag. Vi får ju slita för det här va. Jag, min kollega som har ansvar för informationssäkerhet och min kollega som är dataskyddsombud vi liksom ger och tar av varandra hela tiden. Det dyker hela tiden upp nya saker, men vi har bra struktur. Men sen är det ju problemet med att identifiera informationskällor och sen se till att klassificera dem och vidta åtgärder utifrån eventuella läckage eller juridiska problem.	C06
5	E.M	Vilka steg i det systematiska informationssäkerhetsarbetet har varit mest utmanande?	
6	R03	Ja, det har ju helt klart varit att försöka förstå alla system och digitala informationskällor som regionen förfogar över. Det är ju inte allt som ligger i förvaltning, utan det finns flera system till exempel medicintekniska system som flyter runt lite grann men ändå med personuppgifter i. Så vi håller på med en monumental inventering. Det fanns en inventeringslista men den var ju inte på något sätt tillfredsställande i omfattning.	
7	E.M	Ofta när man pratar om systematiskt informationssäkerhetsarbete så pratar man om att det ska gå i en cirkel. Det tar aldrig slut. Har ni upplevt någon utmaning där med att kanske de system som ni jobbar med som andra förvaltar över att det tar stopp och man glömmer att följa upp i den här processen?	
8	R03	Tveklöst är det så. Vi har infört något som vi kallar Egen kontroll. Det låter kanske larvigt, men där ska varje förvaltning utifrån en rada frågeställningar göra en bedömning av hur man ligger till säkerhetsmässigt i en rad av olika områden och vilken typ man förfogar över. Och där är systemet klassa som du känner till en bra grund att stå på. Så information klassas och sen hoppas vi att egenkontrollerna då rullar in så att vi kan titta på dem och sen följa upp framförallt att åtgärder vidtas. Man får ligga på rätt friskt för att det ska hända någonting.	C06
9	E.M	Jag förstår det. Vad hade underlättat processen för att uppnå ett systematiskt informationssäkerhetsarbete?	
10	R03	Ja, att vi hade inventerat alla våra system och informationstillgångar. Å andra sidan har vi börjat lite clean sheet här faktiskt för det finns ingen tradition i någon region tror jag att hålla koll på saker och ting, men nu är det skarpt läge här utifrån juridiskt ramverk och lokala styrande dokument. Vi har ju till exempel en informationssäkerhets riktlinje. Det låter ju som en rekommendation, men det är beslutat i regionstyrelsen så det är vad som gäller. Och vi har också utbildningar som vi tvingar medarbetare att gå igenom	C01
11	E.M	Då fokuserar vi lite mer på invånartjänster. Här är då första frågan, på vilket sätt inkluderar ert systematiska informationssäkerhetsarbete även invånartjänster, som typ Journalen/1177?	
12	R03	Du menar Journalen på nätet som det kallas?	
13	E.M	Yes.	

14		Det projektet hade faktiskt sin grund i början i Uppsala. Som en studie som sedan blev permanent. Vi har varit med och det har varit en dialog också med sjukvårdsinrättningar. En del har varit väldigt skeptiska, exempelvis psykiatrin på god grund. Jag oroade mig till exempel för unga invandrarkvinnor som skulle ha sina föräldrar, fäderna då företrädesvis, tvingas titta i journalen och det kan ju då ha implikationer då på kvinnosäkerhet. Om en kvinna har varit hos gynekologen till exempel och då uppstår det en allvarlig situation för den unga kvinnan. Så ja, vi har tänkt riktigt ordentligt. Och vi har fått nu också sjukvårdspersonal att acceptera det här och det satt lite långt inne.	C05
15	E.M	Hur har ni styrt det med informationssäkerhet och gjort den kopplingen? Man hade ju lika gärna kunnat göra kopplingen utifrån personsäkerhet snarare än informationssäkerhet.	
16	R03	Ja, absolut. Vi har ju varit med under hela resan då och så att säga inspekterat hur informationsflödena ser ut, hur säkerheten i plattformen ser ut och så vidare. Och riskbedömningar om patienter kan komma att ta ut sina journaler och lägga på sociala medier, vilket tyvärr har hänt. Det är naturligtvis patientens eget fel, men det är ju tragiskt.	C05
17	E.M	Hur ser processen ut rörande informationssäkerhetsarbetet om nya invånartjänster ska läggas till?	
18	R03	Det ser ut på motsvarande sätt. Först är det någon som får en idé, till exempel vi har ju den här mötesplattformen. Vi har en digitaliseringsavdelning som har som uppgift att ta fram nya såna här användartjänster/patienttjänster. Sen går ju det där genom en process där det bedöms om juridiken och av oss på säkerhet och beredskapsenheten. Och där gör vi ju också uppföljningar och det måste vi ju göra nu när den här mötesfunktionen inte innehåller en kommunikationsplattform som håller sig i huset så att säga utan ligger i ett moln. Det håller vi på att ändra på nu. Ingen får ju liksom släppas iväg innan det är noga analyserat.	C06
19	E.M	Vad är de största utmaningarna för invånartjänster i relation till ert informationssäkerhetsarbete/dataskydd?	
20	R03	Det där är en ganska svår fråga. En utmaning är att försöka ha en sansad diskussion om tjänsten faktiskt ger patienten någon reell nytta. Oftast gör det ju det, men ibland kommer det lite väl spejsade idéer som man får hålla emot	C07
21	E.M	Då går vi vidare till att prata om verktyg. Det finns flertalet olika metoder och verktyg för att designa och hantera ledningssystem för informationssäkerhet (ex. MSBs metodstöd, standarder, Klassa, Stratsys). Vilka metoder och verktyg används i ert systematiska arbete generellt?	
22	R03	Pass	
23	E.M	På vilket sätt är de tillräckliga?	
24	R03	Pass	
25	E.M	Vad kan behöva förbättras?	
26	R03	Pass	
27	E.M	Täcker era metoder och verktyg upp även kraven på informationssäkerhet och dataskydd gällande invånartjänster, typ Journalen, eller vad krävs ytterligare?	
28	R03	Yes. Behövs inget ytterligare. Vi bedömer att vi har det vi behöver.	
29	E.M	Sista frågan på det här området gäller GDPR. Och då är jag nyfiken på hur påverkade införandet av GDPR det systematiska informationssäkerhetsarbetet?	
30	R03	Ja, alltså det inleddes med en rätt omfattande panik faktiskt när man insåg att GDPR redan var infört och att vi per definition var olagliga. Det var då också man anställde dataskyddssamordnare och vi har då vår DSO/dataskyddsombudet inom säkerhetsavdelningen. Så det är ett konstant arbete runt om kring. Men vi har fortfarande utmaningar när det gäller GDPR. Jag kan nämna ett exempel som har bollat huvudbry. Det är att region har köpt in insulinpumpar och de där är intelligenta, men för att patienten ska ha nytta av det krävs det att patienten ingår ett avtal med ett amerikanskt företag. Det känns inte klockrent att behöva säga till patienten att ´det är du som ingå avtalet',	C05

		men de anser att de ger ett sådant enormt mervärde att kunna titta på trender och insulinnivåer över tid så att de är villiga. Men det känns inte superbra tycker jag. Många grejer är ju prenumerationstjänster idag på nätet vilket är en ren förbannelse. Man köper ju inte en programvara, utan man hyr den. Men där har vi haft diskussioner med bolaget gällande hur man hanterar informationen, hur den gallras osv. Sen får man på något vis, vi har ju inga regelrätta personuppgiftsbiträdesavtal men något slags agreement i alla fall.	
31	E.M	Spännande. Nästa område berör ansvar och ansvar då i relation till invånartjänster. Vem har ansvaret enligt din uppfattning, för att informationssäkerhet/dataskydd hanteras på ett tillfredsställande sätt gällande invånartjänster?	
32	R03	Det där är inte så lätt att svara på. Om man tittar på journaldata till exempel, vi använder systemet Cosmic, då är det förvaltningen som ansvarar för att överföra data men sen då behöva datan tas emot och där är jag inte helt säker på att gränssnitten är helt definierade. Vi har ett annat system också där man använder patientdata i administrativt syfte och där är det ju också väldigt oklart juridiskt eftersom man går från patientdatalagen till att resonera i termer av administrativ behandling och då blir det frågetecken kring sekretess där.	C04
33	E.M	Kan man gå så långt som att säga att det här ansvaret har hamnat mellan stolarna för att vi skickar data mellan oss på ett helt annat sätt idag i och med invånartjänsterna?	
34	R03	Rent allmänt så skulle man kunna säga det. Inte totalt fullständigt, men i vissa fall finns det oklarheter i ansvarsfrågan.	C04
35	E.M	Nästa område relaterar till användarna som i den här studien inkluderar samtliga typer, exempelvis läkare, sjuksköterskor och invånare. Vilka är utmaningarna kring användarnas kunskap om informationssäkerhet/dataskydd i relation till användningen av invånartjänster kan du identifiera? Ex. är det problem kring att de inte ens känner till att tjänsterna är finns, eller vilken information som är tillgänglig med de här tjänsterna.	
36	R03	Ja, det sista handlar i så fall om invånarna. Att de inte har kunskap om eller uppmärksammat att det går att titta på sina läkemedelslistor, journalen osv. Sjukvårdspersonal är medvetna och man har nu börjat uttrycka sig på ett annat sätt i journalsystemet för att det ska vara begripligt för patienten, men då använder man istället kommentarsfälten i journalsystemet och det är ju inte bra heller. Saker som inte uppenbart ska komma till patientens kännedom som i psykiatriundersökningar till exempel tar man ofta hjälp av anhöriga som då figurer som tredje person i journalanteckningar och det är en komplicerad balansgång. Sen när det gäller GDPR och informationssäkerhet tycker jag att sjukvårdspersonal är bra på att göra bedömningar. Det finns ju folk som försöker runda lite granna, men de får man ta i örat.	C07
37	E.M	Vad är upplevelsen kring samtycke i relation till invånartjänster? Exempelvis när behövs det och när är det snarare rimligt att inte begära samtycke? Här skulle man kunna tänka akutsituationer.	
38	R03	Ja, det är ju akuten i så fall. Vi är ju ett stort universitetssjukhus så det finns en tradition av att inhämta samtycke. Vi har ju del vetenskaplig forskning, men även klinisk forskning inom sjukhuset. Man utbyter då information mellan universitetet och Akies (?). När människor själva ställer upp i forskningsstudie då är det ju lätt, men om till exempel vill ha biomaterial efter en operation för det görs en studie då begär man naturligtvis alltid samtycke. Så det är inget slarv där.	
39	E.M	Vidare, vad är utmaningarna med användarnas beteende i relation till användningen av invånartjänster för upprätthållandet av informationssäkerhet/dataskydd?	
40	R03	Det där vill jag påstå åligger användarna i så fall. Som jag sa, det finns en del Facebookgrupper till exempel Det där håller vi på att diskutera med kommunikationsavdelningen. Där Facebookgruppen is själva verket är startad av anställda men man använder Akies loggen så det ser väldigt officiellt ut. Det har ju hänt då att medborgare ställer frågor om sina sjukdomar i tron om att det är någon slags invånartjänst. jag tror att medvetenheten och självbevarelsedriften är väldigt stor hos invånarna så man är väldigt mån om att vara försiktig med sin information. En hel del vill ju inte ens se sin journal och då låter de bli att öppna den.	C01
41	E.M	Du nämnde att ni har en utbildning som är om jag uppfattat det rätt obligatorisk för sjukvårdspersonalen inom informationssäkerhet?	
42	R03	Ja, alla i regionen.	

43	E.M	Inkluderar det även invånartjänster?	
44	R03	Nej, jag tror inte det.	C01
45	E.M	Inkluderar det beteendet som du beskrev med att använda sociala medier som kommunikationskanal istället för att kommunicera via rätta?	
46	R03	Ja, alltså när det gäller att kommunicera i rätta kanaler det är man medveten om. Just sociala medier, den passagen finns också. Men inte explicit när det gäller invånartjänster men att man inte ska svara på några frågor och helst radera såna som kan vara till nackdel för patienten eller invånaren. Så det är en utmaning. Folk lever ju på Facebook.	C01
47	E.M	Ja, precis. Hur kan dessa utmaningar bemötas? Det låter som att ni har ett bra fokus på sjukvårdspersonal i regionen och så, men invånarna. Går det att bemöta de utmaningarna och invånarnas beteende på något sätt?	
48	R03	Ja, när man loggar in i 1177 får man ju en hel del instruktioner att läsa, vad det innebär att använda dessa invånartjänster och sedan ska man trycka på lilla plutten att man tagit del av informationen. Så förhoppningsvis, jag tror att folk läser det där. För man kommer ingenstans om man faktiskt inte engagerar sig. Men det är klar det finns säkert folk som bara klickar hej vilt i vanlig ordning, men vi har försökt göra det vi kan	C07
49	E.M	Nästkommande frågor berör tillgång och behörighet. Hur hanteras konflikter mellan behörighetsbehov ex. akuta situationer och att upprätthålla dataskyddet i relation till invånartjänster?	
50	R03	Ja, det där är en komplex fråga. När det gäller behörighetsbehov så har ju akuten alltid override och det kan ju handla om patientens liv. Kommer in medvetslös och tar en viss medicin så medicin mot högt blodtryck och sen så kommer man inte åt journalen och sätter in medicin mot högt blodtryck då kan ju patienten per definition dö. Så akuten får alltid göra override. Sen röntgen också. Lite speciella, de är ju en konsultativ verksamhet. De får en remiss och anamnes och ska då ta ställning, sen ska de också lämna ett svar. Så de har ju höga behörigheter naturligtvis och ska ha annars funkar det ju inte. Du är säkert familjär med att en invånare också kan spärra sin journal. Det där tycker jag är lite spel för galleriet, visserligen det är inte så att sjukvårdspersonalen inte kommer in i den spärrade delen av journalen med däremot kommer det upp en skylt som informerar att patienten betraktar det som spärrad information. Och den bedömningen har man gjort för att det kan medföra väldigt stor patientfara för ibland har vi sett att patienter liksom spärrar olika delar som gör att det inte går att bedriva någon vård. Spärra bort röntgen till exempel är inte någon bra idé.	
51	E.M	Du lyfter upp en bra poäng där för följdfrågan jag hade var om det är en konflikt och utifrån ditt svar så är det en konflikt, men man har inom sjukvården kunnat lösa det så att de som behöver akut access får akut access för det finns ett reellt behov för det. Men då kanske det finns en konflikt mellan invånarnas upplevelse av behörighetsbehov och deras förmåga att kunna spärra. Vilket man löst med att de kan spärra, men det är inte faktisk spärr såtillvida att sjukvårdspersonal inte kommer åt informationen.	
52	R03	Däremot kan man ju sätta en verklig spärr på att tanka upp grejer i nationell patientöversikt. Som jag personligen tycker är ett overlskt (?) system, men där går det att sätta en reell spärr.	
53	E.M	Gällande behörighetsansvar. Vem ansvarar för att behörigheterna är lämpliga i relation till invånartjänster?	
54	R03	I princip är det förvaltningen som hanterar eller har hand om de system som innehåller en viss information. Naturligtvis försöker vi följa upp det där. Vi håller också på med ett bronto projekt där vi verkligen ska gå igenom behörigheter. Det är inte bara till såna här system som det är en problematik. Människor byter arbetsuppgifter, går till en ny avdelning men behåller de gamla behörigheterna. Så just saneringen av tidigare behörigheter behöver förbättras.	C06
55	E.M	Vem ansvarar för att kontrollera att behörigheterna hanteras korrekt i relation till invånartjänster?	
56	R03	Det gör respektive förvaltning. Naturligtvis man kan hårdra allting till att det är regiondirektören som har yttersta ansvaret, men det är lite väl högt upp faktiskt. Eller egentligen är det regionstyrelse, vi är ju en politiskt styrd organisation. Men det ligger på rimlig nivå och sen görs det stickprovs analyser osv. Något vi använder väldigt flitig i regionen är riskanalyser och sen att vi fattar beslut utifrån vad som kommits fram till under riskanalyserna. Och att man också inte startar någon ny funktion eller tjänst om	C06

		det inte är så att allt som hamnade på rött är åtgärdat.	
57	E.M	Låter som en rimlig hantering.	
58	R03	Ja, och det är faktiskt så att nu är förfrågningarna från alla möjliga att få riskanalyser genomförda så till den grad att vi måste försöka få mer folk som kan ägna sig åt det. Och det kan man ju säga är en framgångsfaktor. Hade det inte kommit från förfrågningar om riskanalyser då var det ju ingen som brydde sig.	
59	E.M	Härnäst kommer ett par frågor om de standarder som berör informationssäkerhet och dataskydd. Först och främst, ISO 27000-serien så du säker känner till väl	
60	R03	Ja, övergripande. Jag kan ju inte referera till olika delar i den.	
61	E.M	Det förstår jag. Frågorna är, underlättar eller försvårar dessa standarder ert systematiska informationssäkerhetsarbete? Och är det något som behöver bli bättre i dem?	
62	R03	Du menar i standarderna?	
63	E.M	Ja.	
64	R03	Alltså vi har ju ett öga på ISO 27000-serien, men följer inte den slaviskt. Det är mer en inspirationskälla, sen lutar vi oss mot det som vi har tagit fram men är det så att vi upptäcker att vi har missat någonting som är relevant för sjukvården då tittar vi på det.	C06
65	E.M	Men ni upplever dem ändå som begripliga och lättförståeliga? För det är ju inte helt ovanligt att man tycker att standarder är högtravande.	
66	R03	Högtravande är det ju absolut. Det är ju inte nödvändigtvis så att det är lätt att förstå. Det där är ju för att hoppa över till GDPR som reflektion. Den skrevs ju på ett sätt som skulle göra den begriplig för alla och envar. Jag tycker man lyckades väldigt bra. ISO standarder är ju väldigt träiga.	C01
67	E.M	Utöver 27000-serien finns också ISO 27799 som är en förlängning av 27000-serien specifikt för hälso- och sjukvård. Underlättar eller försvårar denna standard ert informationssäkerhetsarbete? Och är det något som behöver bli bättre?	
68	R03	Vad som behöver bli bättre kan jag faktiskt inte bedöma för det skulle vara då att vi hade lusläst just den här, men det är också en slags inspirationskälla kan man säga. Vi följer det inte slaviskt utan vi försöker hålla oss så nära verkligheten som möjligt för vi skulle liksom inte komma någonstans om vi kom dragande med en massa ISO, kommunicerade dessa med verksamheterna. Men däremot inom säkerhets och beredskaps avdelningen är vi naturligtvis om dem.	C06
69	E.M	Till sist finns ISO 27701 som är en förlängning av ISO 27001 och berör insamling samt hantering av personuppgifter. Den togs fram just för att en del hade svårt att förstå GDPR som alg och vad det innebar. Underlättar eller försvårar denna standard ert systematiska informationssäkerhetsarbete? Vad behöver bli bättre?	
70	R03	Jag ska vara helt ärligt. Vi har inte tittat så mycket på den för vi är swamped in GDPR problematiken.	C05
71	E.M	Ni behöver den kanske inte?	
72	R03	Nej, vi har inte upptäckt det än i alla fall. Däremot har vi varit ganska framgångsrika, och det är ju dataskyddsombudet och juristerna som ska ha cred för det, i kommunikationen vad GDPR faktiskt har för implikationer på det vi gör. Så man får äta elefanten i små tuggor i taget.	
73	E.M	De följande två frågorna berör de olika typerna av applikationer. Först, vilka utmaningar som din region ser med ert systematiska informationssäkerhetsarbete i ökningen av mobila enheter?	
74	R03	Det här är ju ett problem. Pratar du om regionanställda som använder appar eller invånare?	
75	E.M	Du kan få ta båda.	

76	R03	Ja, vi har ju tagit ett grepp när det gäller mobila enheter som är av tjänstekaraktär. Att man inte kan installera vilka appar som helst och vi har också sett till att vissa yrkesgrupper inte heller kan ta bilder vissa tider på dygnet för att det inte ska fotograferas på sjukhuset. Det är totalt förbjudet. Däremot är det några som har tillstånd när det gäller att dokumentera och sen lägga in i journalsystemet. Det där tror jag är ett problem för alla företag. Jag var på Sveriges radio innan och det var en kamp att få användare att förstå att man ska inte installera vad som helst. Många appar till exempel TikTok som jag lyckades få förbjudet på Sveriges radio, som jag är hemskt nöjd med, suger ju i sig kontaktböcker och allting och där kan det ju va konfidentiella kontakter. Så mobila enheter är ett mörker faktiskt. Datorer har vi örnkoll på, men en del tar ju tjänstesimkortet och sätter i den privata telefonen och då är man ju rökt igen.	C04
77	E.M	Hur påverkar dessa mobila enheter hanteringen av dataskydd?	
78	R03	Det är inte så att du menar tvärtom? Dataskydd påverkar mobila enheter?	
79	E.M	Den tolkningen får ju gärna göra också om du vill.	
80	R03	Hanteringen av dataskydd. Nu pratar jag om hur det står här [Hur påverkar dessa mobila enheter hanteringen av dataskydd?]. Det blir ju en utmaning i och med att vi inte kan garantera att det är tjänstemobiler som är styrda enligt vissa behörighetsgrupper. Och det här med att folk sätter tjänstesimkortet i privata mobiler det är ju rätt så hopplöst att komma åt. Däremot kommer man inte in i det inre nätverket om man fuskar med såna fasoner därför att tjänstemobilerna har ju såna här certifikat som kan autentisera mot trådlöst nät och så vidare. Så det är säkerhet i sig. Men fortfarande kan det vara så att det finns olämpliga uppgifter i en privat mobil då en hel adressbok till exempel I regionen har ju det flesta läkarna dolt nummer för det inträffar ibland direkt hot, överfall faktiskt från patienter, tyvärr uteslutande inom psykiatrin men i alla fall. Det finns rättshaverister i andra sammanhang också så de måste skyddas.	C04
81	E.M	Härnäst är jag intresserad av ditt perspektiv på hot kopplade till invånartjänster. Vilka är de främsta hoten med invånartjänster?	
82	R03	Rent allmänt så är antagonistiska hot, de kan vara statsunderstödda eller kriminella nätverk, det som bekymrar mig mest. Kanske inte just med invånartjänster men i förlängningen det som finns bakom. Det är ju ingen hemlighet att Ryssland nu har börjat med en offensiv när det gäller rena cyberattacker, påverkansoperationer, desinformation och så vidare. Jag brukar säga att en bank som blir rånad på 40 miljoner det är kanske tråkigt, men det kan skrivas om som en kapitalförlust. Däremot skulle vi läcka ut det allra minsta om en patient så skulle det kunna ha oerhörda konsekvenser för den individen. Och en utmaning i alla sammanhang är hanteringen av skyddade identiteter. Men att man ger sig på 1177 och knäcker sig vidare in, det är inte så troligt. Det är svårt, inget är omöjligt men det blir ett ordentligt bökande i så fall.	C04
83	E.M	Och de här hoten, hur påverkar de ert systematiska informationssäkerhetsarbete/dataskydd?	
84	R03	Asså, vi försöker ju vara proaktiva här. Mitt arbete till exempel går till viss del ut på att försöka tänka ut vad som kan hända, hemskt redan innan det händer. Försöka hitta några mitigeringsåtgärder då för att komma tillrätta med det. Så visst påverkar det vårt informationssäkerhetsarbete, cybersäkerhet och dataskydd. Vi är ju en trojka just för de här tre och det funkar väldigt bra.	C04
85	E.M	De sista frågorna berör framtiden. Då undrar jag hur ser du på framtiden och kommande invånartjänster? Jag lägger upp följdfrågorna här direkt. Hur kompletteras det systematiska informationssäkerhetsarbetet för att inkludera nya tjänster? Hur kommer nya tekniker ex. molnlösningar påverka det systematiska informationssäkerhetsarbetet/dataskyddet?	
86	R03	Asså, jag kan börja med molnlösningar. Det är ju liksom en paria. Det finns ett fenomen. Läkare är på olika konferenser och hittar system som de tycker skulle förbättra arbetet och så köper de in det där i strid med upphandlingsreglerna och sen står man där med ett system som till exempel pumpar över data till tredjeland. Inte en höjdare. Och hur det systematiska arbetet kompletteras, asså vi försöker ha en dialog. Det är väldigt mycket hittepå i regionen. Det gäller att ha de coolaste invånartjänsterna och sådär, men om man analyserar ordentligt och faktiskt tar fram lösningar som har reell nytta, för det är inte alltid så, då har vi ju en chans att komma in i arbetet på ett helt annat sätt än att det dyker upp. Om man inte tar hand om såna här frågor innan så är det praktiskt taget omöjligt att få ordning på sen. Och en av huvudvärkarna är nämligen olika molnlösningar. Där ökar medvetenheten hos regionens anställda och sjukvårdspersonal väldigt mycket faktiskt. Man börjar faktiskt ta till sig problematiken med det här. Däremot moln inom Europa får man teckna avtal som är i paritet med lagstiftningen och personuppgiftsbiträdesavtal osv. Det brukar inte vara något problem om det är seriösa företag man har att göra med.	C04, C07

87	E.M	Avslutningsvis, är det något mer du vill tillägga som rör utmaningar gällande ledningssystem för informationssäkerhet eller dataskydd som relaterar till användningen av invånartjänster?	
88	R03	Inte vad jag kan komma på just nu faktiskt. Det dyker upp nya saker hela tiden, men just nu kan jag inte komma på något.	
89	E.M	Finns det andra utmaningar gällande ledningssystem för informationssäkerhet eller dataskydd som du/ni vill lyfta som inte berör invånartjänster?	
90	R03	Det är ju att få organisationens förståelse för hur informationssäkerhetsarbete bedrivs och vilka verktyg man använder och varför. Det är utmaningen skulle jag vilja säga. Men samtidigt är jag positiv i den bemärkelsen att det går bättre och bättre. Det har varit oerhört kämpigt länge, men nu börjar förståelsen falla på plats och då kan man använda ledningssystem och hänvisa till det.	C07