TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Ieva Marija Kuzminaite 182581YVEM

A qualitative approach on the viewpoints of different stakeholders regarding information security and data privacy in terms of healthcare service provision

Master's thesis

Supervisor: Hedvig Soone
Msc

Co-Supervisor: Kadi Lubi
PhD

Tallinn 2023

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Ieva Marija Kuzminaite 182581YVEM

Erinevate sidusrühmade vaatepunktide kvalitatiivne analüüs infoturbe ja andmete privaatsuse tervishoiuteenuse osutamise kontekstis

Magistritöö

Juhendaja: Hedvig Soone
MsC

Kaasjuhendaja: Kadi Lubi
PhD

Tallinn 2023

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Ieva Marija Kuzminaite

11.05.2023

Abstract

Background: With a growing rate of electronic health data sharing, ensuring information security and data privacy is critical for all healthcare organisations. For many years Estonian healthcare providers have had to implement information security and data privacy related requirements in their organisations. During 2023 Estonian healthcare providers will have to transition from currently valid information security standard ISKE to a new standard called E-ITS. As implementation of changes in IT and digital innovations has been perceived as very disputed area in healthcare, effective change management for that is required. **This thesis aims** to identify the viewpoints of different stakeholders regarding information security and data privacy in terms of healthcare service provision in the context of change management. **Methodology:** A qualitative secondary data analysis from the semi-structured interviews led by the NORDeHEALTH team was conducted. Thematic textual analysis was performed, and both deductive and inductive coding methods were used for analysing the data. **The results** revealed three main thematic categories: general experiences with information security and data privacy requirements, supporters and barriers for implementing and complying with information security and data privacy requirements. Firstly, good preparation and communication must be prioritized before IT-related change implementations to reduce resistance. Secondly, continuous trainings, good communication between organisations, personal motivation and organisation's support were the main supporters mentioned. Thirdly, main barriers identified were lack of resources, resistance to information technology, human behaviour, and responsibility for compliance which can eventually all lead to negativity towards information security and data privacy compliance. **Conclusions**: Although there are several supporting actions and activities identified that make change implementation an easier process, there are more barriers that should be addressed and solved to facilitate the process of change management. Using change management models is strongly advisable for successful change implementation process in healthcare providers.

This thesis is written in English and is 49 pages long, including 6 chapters, 1 figure and 2 tables.

Annotatsioon

Erinevate sidusrühmade vaatepunktid infoturbe ja andmekaitse kohta tervishoiuteenuse osutamisel

Taust: Elektrooniliste terviseandmete jagamise kasvu tõttu on oluline tagada infoturve ning andmete privaatsus tervishoiu organisatsioonides. Eesti tervishoiuteenuse osutajad on rakendanud infoturbe ning andmete privaatsusega seotud nõudeid oma organisatsioonides aastaid. 2023 aastal peavad Eesti tervishoiuteenuse osutajad üle minema praegu kehtivalt ISKE infoturbe standardilt E-ITS standardile. Kuna digitaalsete ja IT-alaste muudatuste rakendamine tervishoius on tekitanud vastuseisu, on oluline antud muudatust efektiivselt juhtida. **Uurimistöö eesmärk** on tuvastada erinevate sidusrühmade vaatepunktid infoturbe ja andmekaitse kohta tervishoiuteenuse osutamisel muudatuste juhtimise kontekstis. **Metoodika**: teostati kvalitatiivne teisene poolstruktureeritud intervjuude analüüs. Intervjuud viidi läbi NORDeHEALTH meeskonna poolt. Intervjuusid analüüsiti temaatilise sisuanalüüsi meetodil, kombineerides deduktiivset ja induktiivset kodeerimist. **Tulemused** tõid esile kolm peamist teemakategooriat: üldised kogemused, toetavad ning takistavad faktorid infoturbe ning andmete privaatsuse nõuete rakendamisel ja täitmisel. IT-ga seotud muudatuste rakendamisel tuleks prioritiseerida ettevalmistus ning kommunikatsioon vältimaks vastuseisu. Protsessi toetavateks faktoriteks olid pidevad koolitused, hea kommunikatsioon organisatsioonide vahel, isiklik motivatsioon ning organisatsiooni toetus. Takistavate faktoritena tuvastati ressursipuudus, vastuseis IT-le, inimkäitumine ning vastutus nõuete täitmise eest, mis võivad viia negatiivsete hoiakuteni seoses nõuetega. **Järeldused:** Kuigi tuvastati mitmeid toetavaid faktoreid, mis lihtsustavad muudatuste juhtimist, on muudatuste elluviimise protsessis ka takistavaid faktoreid, mida silmas pidada muudatuste protsessi hõlbustamiseks. Tervishoiuteenuse osutajatel on eduka muudatuste rakendamise protsessi tagamiseks soovituslik kasutada muudatuste juhtimise mudeleid.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 49 leheküljel, 6 peatükki, 1 joonist, 2 tabelit.

List of abbreviations and terms

EHR	Electronic Health Record
EU	European Union
E-ITS	Estonian Information Security Standard
ENHIS	Estonian National Health Information System
GDPR	General Data Protection Regulation
HIPAA	The Health Insurance Portability and Accountability Act
HIT	Health Information technology
IEC	International Electrotechnical Commission
ISMS	Information Security Management System
ISKE	Estonian IT baseline security system valid till 2023
ISO	International Organization for Standardization
IT	Information technology
PDPA	Personal Data Protection Act
TalTech	Tallinn University of Technology

Table of contents

List of figures

List of tables

1 Introduction

Information technology (IT) developments with digitization of health records have made it possible to improve the means of efficiently and effectively collect, process, store, consult and share patient health information [1]. The use of electronic health records (EHRs) has grown significantly over the past 10 years [2]. EHRs are digital forms of patient records that include patient information such as contact information, patient's medical history, allergies, test results and treatment plan [3]. EHRs are expected to increase efficiency in healthcare delivery and improve healthcare quality. At the same time perceived vulnerability of EHRs to security concerns of health records databases has emerged [2]. There have been multiple concerns about the impact of digitalization on information overload and uncertainty, interaction with patients, privacy issues, disruptions to workflows, and increasing workflows, which can all contribute to different mistakes [4]. A rise of data security incidents is a growing threat to the whole healthcare industry and to healthcare organisations in particular [5] [6]. As a result of that, patients but also healthcare professionals can be reluctant to widely use some health information technology (HIT) functionalities like health information exchange, telehealth and mobile health which could ultimately result in ineffective health care delivery, ineffective health monitoring or health research [1] [2] [7] [8].

Ensuring information security and data privacy is critical for all healthcare organisations [9]. Various laws, regulations, standards, systems, and rules have been developed and applied to healthcare organisations to ensure that the patient's health data would remain private and secure [10]. Still, there are researches claiming that IT-related security and privacy measures are quite poor in many European and American healthcare providers [1] [11]. It is important to understand the problems healthcare providers are facing and how they are perceiving all the security and privacy related requirements that they should comply with.

Different IT implementations in hospital settings have a strong influence on whole organisations and its employees. A study by Hospodkova et al. has stated that more than

80% of hospital personnel have indicated that the most disputed area of changes is the implementation of changes in IT and digital innovations [12]. Changes or implications can be perceived meaningless and unjustified when the need of the change is not understood, which can create change resistance in the organisation [6]. As different regulations and requirements often come outside the organization, the way changes are implemented and communicated are especially important [6].

Like in many other countries, Estonian healthcare providers have had to implement information security and data privacy related requirements in their organisations due to national information security standard and General Data Protection Regulation (GDPR) [13]. As many Estonian healthcare providers are publicly owned private hospitals with self-governing trusts [14], they are responsible for compliance with all national requirements. While GDPR is valid from May 2018 and respective local regulation Personal Data Protection Act is effective as of year 2019 [15], Estonian healthcare providers among many other organisations have to switch from currently valid information security standard ISKE - Estonian three-level IT baseline security system (*Infosüsteemide kolmeastmeline etalonturbe süsteem)* to a new standard called E-ITS – Estonian Information Security Standard (*Eesti Inforturbestandard*) by the end of 2023 [16]. This means that management of the hospitals must allocate resources, organise the workflow, provide correct systems, train medical staff etc to incorporate all the required changes. Effective management is required to facilitate change and achieve results through ensuring the efficient utilisation of the health workforce and other resources [17].

The aim of this study is to identify the viewpoints of different stakeholders regarding information security and data privacy in terms of healthcare service provision in the context of change management.

This thesis has six chapters. The first chapter is an introduction about the research topic. The second chapter describes the background of information security and data privacy aspects and regulations, gives an overview of Estonian National Health Information System and describes change management and its theories in healthcare. The third chapter consists of research problem and presents the research questions. The fourth chapter describes the methodology and the methods used for analysing the data for this study. Chapter five shows the results, and the sixth chapter discusses the results. Eventually the seventh chapter shortly summarizes the whole research.

2 Background

This chapter gives an overview about the background of information security and data privacy aspects, including the principles of information security management system, Estonian National Health Information System and the regulations and requirements that are relevant in the context of this study. Due to latter, change management theories in healthcare are also described in this chapter.

2.1 Information security and data privacy

2.1.1 Patient's health data

Health data is an information related to the past, current, or future physical or mental health status of a person, that is captured by health-care professionals and, mostly recorded and stored in patient's electronic health records (EHRs) [18]. A patient's health data is highly private and sensitive [2]. Negligence and reporting errors on patient health records might change the treatments and can cause patient harm [19]. Good management of patient medical records protects patients and builds trust in healthcare provider, as well as protects physicians and hospitals against claims of negligence [7] [2]. As health data is quite complex, meaning that health data often resides in multiple places, occurs in different formats, is both structured and unstructured [20], maintaining the trustworthiness of health data is a considerable challenge [21]. Additionally, the increasing size of health data, distributed storage of health data at different places and a big number of data sources adds extra difficulties and complexities for keeping that trustworthiness [21].

Data breach is generally an illegal disclosure or use of information without an authorization [22]. Healthcare data breaches can harm both individuals and organisations and they are categorized in two major categories: internal and external. In the US alone, the total number of healthcare records that were exposed, stolen, or illegally disclosed in 2019 was 41,2 million from 505 healthcare data breaches [22]. Even though European

healthcare systems differ often from American healthcare systems [11], data breaches are still prevalent all over the world [22].

An analysis from 2019 based on IT security and privacy practices from 1723 European hospitals from different regions has shown that around 70% of those hospitals failed to implement basic security and privacy measures consistent with their digitization level [1]. Even though hospitals have increased their IT security during digitalization period, the enhancement of IT security and privacy practices as the health information digitization advances have been reported neither systematic nor strong enough [1].

Researches, both quantitative and qualitative, show that physicians are involved in frequent data breach incidents by making very simple mistakes due to lack of knowledge about patient confidentiality aspects such as disclosing medical information to third parties [2] [7] [9]. Studies that investigate the factors that contribute to ethical misconduct and the impact of continued ethics education on physicians' knowledge and practice are lacking and recommended for conducting [14]. Confidentiality concerns have been acknowledged as being global concerns. Therefore, various recommendations and guidelines that apply to protecting the virtue of patient's private lives during treatment have been developed [9].

2.1.2 Information security management system

An information security management system (ISMS) is a systematic approach to manage sensitive information through people, processes, and IT systems [7]. The goal of an ISMS in healthcare is to ensure that information is protected from unauthorized access, use, disclosure, modification, or destruction [1]. The components of securing information assets include software, hardware and human awareness and the key characteristics of the information security are confidentiality, integrity, and availability that all need to be managed properly throughout every healthcare organisation [7].

There are many different information security standards that are being used [23]. Some standards for information management systems are for example ISO 9001, ISO 14001, OHSAS 18001/ISO 45001 and ISO/IEC 27001 which is claimed to be the leading international standard for information security management [24]. The ISO/IEC 27001 was designed and published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) as an evolution of BS 7799 – a

standard developed by the British Standards Institution [25]. ISO/IEC 27001 provides a model for establishing, implementing, operating, monitoring, reviewing, and improving ISMS [23]. Mandatory standards that are applied in Estonian organisations are elaborated in chapter 2.2.2.

Information security is achieved by implementing a set of countermeasures or controls to ensure the integrity and security of the information healthcare organisations use to make critical business decisions [7]. This could be both organisational countermeasures like policies and procedures and technical countermeasures like software functions [7]. Very important aspects of EHR systems are privacy, security, and confidentiality [3]. Privacy refers to a moral right for patients to determine when and how their private information is accessed and shared [2]. The security of EHRs involves protecting the data and security resources, including how data is stored and transmitted across computer systems [2]. Confidentiality involves protecting data from access by unauthorized people through the process of storage, transmission and when the patient is receiving care [2].

2.2 Data protection regulations

Data privacy and data protection are two interrelated issues that are often used as synonyms. Data protection is a legal mechanism that ensures privacy meaning that data privacy defines who has access to data while data protection provides tools and policies to actually restrict access to the data [26]. Regulations on data privacy and data protection policy enforce a set of obligations to organisations [8]. Ensuring patient privacy and protecting personal data is one of the key elements in building patient trust in the employees and the healthcare organisation [8]. Healthcare providers have to pay close attention to the evolving regulatory environment in the country [27]. In developed countries, there are data privacy and protection laws implemented to securely process patient's personal data [28]. Some of the regulations have been brought out in the next subsection. Even though most healthcare providers in developed countries are officially in compliance with the privacy regulations and data security requirements stipulated by active regulations, data breaches still occur among employees [28].

2.2.1 The European Union General Data Protection Regulation

There is a high dependency on sensitive information with respect to patients' personal health which can trigger data security problems. Often in healthcare organisations vast

amount of personal and health data have been collected [29]. One of the most recent important legislations on data protection is the European Union General Data Protection Regulation (GDPR), which passed in April 2016 and came into force in May 2018 across the European Union [29].

In Europe, the operational activities in healthcare organisation must comply with the GDPR [30]. The GDPR addresses the protection of data subjects with regards to the processing and of their personal data. In order to secure their personal data, the legislation introduced a set of rules across EU countries and its citizens irrespective of being located within or outside the European Union [30]. Additionally, there is a "special category of personal data", under which health data is categorised. This category has even more strict regulations for defining and processing sensitive personal data [31]. Nevertheless, the provisions of the GDPR are quite general and lack the specifics needed for routine implementation, leaving room for member states to modify certain aspects of the GDPR in their own data protection laws, especially in healthcare that require more detailed provisions [8].

2.2.2 Health Insurance Portability and Accountability Act and California Consumer Privacy Act

In the United States, The Health Insurance Portability and Accountability Act (HIPAA) provides federal protections for electronic patient health information by ensuring both privacy and security of identifiable health information [2]. While HIPAA is predominantly an insurance legislation, the HIPAA Privacy regulations for how covered entities must protect individually identifiable health information, called protected health information (PHI) [32].

In 2018, California legislators passed the California Consumer Privacy Act (CCPA), which is a digital privacy regulation conferring consumers more control over their online personal information [33]. Although CCPA is a California law, it imposes very strict requirements on businesses nationwide, including healthcare organisations which gather personal healthcare data from Californians. Similarly to GDPR, CCPA is a strict law that is considered to be the toughest and most comprehensive data privacy law in the US [33].

2.3 Data exchange in terms of healthcare service provision

Estonia's digital health system is an innovative example of how technology can be used to improve healthcare [34]. Estonia has established its National Health Information System (ENHIS) already since 2008 which has developed largely and implemented various e-services during those digitization years [35]. Its aim was to make all health information available to patients and health professionals [36]. ENHIS is a standardized information-exchange platform that connects all providers and allows data exchange with other sources [35]. The data is personalised and allows people to access their own health data. It is possible to allow or deny an access to their health data for health care professionals to use in treatment [36]. Although Estonian eHealth system is much broader and consist of many different parts and participants, this research focuses mostly on the tasks of Estonian National Health Information System that stores centrally care summaries and serves as a coordinating tool for the health system, connecting providers across levels of care and between disciplines [37]. Therefore, author does not present any other aspects of eHealth system in this research.

Data exchange between private and public sector organisations is provided by a state-managed central data exchange X-road which enables different information systems to link [38]. The main working principles of X-road are security, standardization, traceability, and verifiability [36] and it is proved to be scalable, transparent, trustworthy, efficient and can work across all sectors [39]. Estonia uses national ID card and blockchain technology to ensure security, legitimacy, and lawfulness of data exchange, keeping track of data access and improving data integrity [21]. Estonia has not limited itself to the initial e-Health initiatives but continues to expand its research and aims at continuous development of the e-Health system, collaborating with key stakeholders across academia, industry, and the IT sector [40].

2.3.1 Regulations and requirements for healthcare providers

In Estonia, healthcare providers are autonomous entities who operate under private law. Most hospitals are either limited liability companies owned by local governments or foundations established by the state, municipalities, and other public agencies. Most ambulatory service providers are privately owned [36]. Legislation obliges all health service provides to submit relevant medical information to the central health information system (CHIS) and providers can also use its health data of their patients [36]. The Law

of Obligations Act [32] defines the legal relationship between the patient and the doctor and requires the involvement of patients in decisions regarding their own health. Health care providers need written informed consent to be signed by the patient before providing any health service [36]. The collecting, managing, and analysing the personal health data in Estonia is regulated by the Personal Data Protection Act [42] and the implementation surveillance is the responsibility of Estonian Data Protection Inspectorate [36].

Estonia enacted new Personal Data Protection Act (PDPA) in 2019 for the purposes of implementing the provisions of GDPR into Estonian law [15]. Both GDPR and the PDPA apply to data controllers, data processors, data recipients, data subjects and third parties, who are authorized to process personal data. Estonia's PDPA established some exceptions to the general principle of the processing of personal data for journalistic, scientific and research purposes [15]. The law also establishes the general principles of which law enforcement agencies must base their actions in processing data [43].

Currently all public organisations in Estonia, including hospitals, are obliged to use information security standard called ISKE which is based on German information security standard – IT Baseline Protection Manual [44]. The standard has a three-level baseline system. ISKE information system will remain valid until 31st December 2023 [44]. From 1st January 2024 a new Estonian information security standard called E-ITS will be mandatory for all organisations fulfilling public duties [16], under which all healthcare providers also are categorized. This means that all ISKE users will have to transfer to the new information security standard by that time [16]. E-ITS is based on German BSI IT-Grundcschutz baseline security method and EVS-ISO/IEC 27001 standard and its aim is to develop and promote the level of information security [45]. The management of all the relevant organisations is responsible for the implementation, maintenance, and improvement of all information security activities [45].

2.4 Managing change in healthcare

The goal of an ISMS in healthcare is to ensure that information is protected from unauthorized access, use, disclosure, modification, or destruction. This can be achieved through the use of technical controls such as encryption and access controls, as well as non-technical controls such as policies and procedures for handling sensitive information.

Both control systems require organisational change management to be implemented successfully. [46].

A conducted study claims that “86% of respondents in healthcare organisation indicated that the most contentious area of changes is the implementation of changes in IT and digital innovations” [12]. It is important to recognise that individuals play a critical role in the success or failure of organisational change. Human dimension is the primary criticality to be managed [47]. Change acceptance is a key factor in the process, and healthcare professionals are not passive recipients of change. In fact, their behaviour can greatly impact the success or failure of a change initiative [48] [49]. It is important to recognize that change is a process, and individuals may go through different stages as they adapt to the new situation [47].

Often many cases of organisational change in healthcare have been in the form of externally initiated reforms which are almost solely implemented through top-down processes [48]. A study in Finland has shown that physicians were less satisfied after implementing a new EHR in their organisation mostly because of increased workflow disruptions [4]. More disruptions were noted during the transition period and after several months the situations recovered [4]. In these change processes, healthcare managers become the intermediaries and implementers of changes that neither they nor other staff member recognize as addressing the relevant problems in their organisations. As a result, the suggested solutions are often experienced questionable or as a poor fit and that is why many reforms of this type have not been particularly successful in the eyes of the staff and in long term effects [38].

2.4.1 Complexity of change management in healthcare

Change involving reorganisation in healthcare organisation is a process of complex dynamics [48]. This is because healthcare settings typically involve multiple stakeholders with different perspectives, priorities, and goals - healthcare organisations must balance the needs of patients, providers, payers, regulators, and other stakeholders, which can create conflicting demands and expectations [46]. In order to effectively manage organisational change, it is important to healthcare organisations to have a clear understanding or the drivers of change and to develop a strategy for implementing the necessary changes [47].

Peter Drucker was one of the first persons to develop ideas for the effective management of organisations [50]. Drucker did observe that healthcare organisations are among the most complex organisations to manage [51]. Drucker describes difficulties in healthcare management as a "two-headed monster", due to the fact that there are two different professional aspects in given sector – medical and non-medical [50]. Medical professionals are more familiar with biomedicine and knowledge that non-medical professionals. On the other hand, non-medical professionals are also qualified and are educated in managing different functions or organization and work with a broader perspective [51]. Even though advances in knowledge and medical technologies have increased the capability to tackle complex health needs, the integration of updates into existing healthcare management practices requires strong change management [51].

2.4.2 Implementation of change management theories in healthcare

Change is a continuous feature in organisational life and successful organisations, , where managers are required to have competency in managing organisational change [52]. It is a common assumption that the style of management is a key factor in the success or failure of organisational change. A significant problem specific to healthcare is that almost two-thirds of all change projects fail [53]. Different management styles can have a significant impact on the way that change is implemented and how it is perceived by employees and other stakeholders [46]. There are number of theoretical approaches that have been developed to guide the process of organisational change in healthcare organisations [48]. These approaches typically focus on the identification of the drivers of change and the development of a plan to address those drivers in a systematic and coordinated manner [47].

Change management models provide a frame of reference for change agents to support them to consider key elements required for change to occur and be sustained [54]. The key elements of that include exploring why the change is needed and crafting the right messages for stakeholders at every step to bring them along on the change journey [54].

Effective management is required to facilitate change and achieve results through ensuring the efficient utilisation of the health workforce and other resources [17].

Table 1. Steps of change management theories [53] [55]

Lewin's Theory of Planned Change, 1947	1. Unfreezing	2. Moving	3. Refreezing
Lippitt's Phases of Change Theory, 1958	1. Becoming more aware of the change	3. Defining change problem	6. Maintaining the change
	2. Developing relationship between system and agent	4. Setting change goals and action plan for achievement	7. Terminating the relationship with change agent
		5. Implementing the change	
Rogers' Diffusion of Innovation Theory, 1962	1. Educating and communicating to staff about the change	3. Staff decision to accept the change	5. Confirmation and usage from the staff
	2. Persuading the staff	4. Implementation of the change	
Kotter's Eight-Step Model of Change, 1995	1. Creating sense of urgency	4. Communicating vision	7. Building on the change, sustaining it
	2. Forming a guiding coalition	5. Removing change barriers	8. Making the change stick
	3. Creating vision	6. Providing short term wins	

There are couple of change leaders and theorists that have contributed to change management with their works more than others [53]. Lewin was an early change scholar who proposed only a three-step process for ensuring a successful change. Later theorists like Lippitt, Kotter and Rogers have added to the collective change knowledge to expand (Table 1) upon Lewin's original Planned Change Theory [53].

Lewin's Theory of Planned Change developed in 1947 and it includes three stages: unfreezing, moving and refreezing meaning that there should be an understanding that change is needed and resistance is broken, followed by the process of initiating change and finally establishing a new status quo [53]. Lewin referred to social habits, which play a major role in preventing change as an *inner resistance* to change and in order to

overcome it, it is necessary to apply an additional force that is sufficient to break the habit or 'unfreeze' the custom [55]. Lewin's theory states that the key to a successful implementation of change is clear communication of the vision and desired changes. Additionally, he has emphasized that there are two types of forces of associated change – driving forces and resisting forces, where first are the change facilitators and the latter are factors that hinder the change. In order to achieve the desired change, driving forces should outweigh the resisting forces.[56]. Lastly, the leaders of the change should support employee's involvement in every step – leaders should educate, provide emotional support and incentives, communicate and co-optate the employees about the change [57].

Other theorists have brought out more stages in their change management theories. Lippitt created the Phases of Change Theory in 1958 that encompasses following change plans: 1) becoming more aware of the need for change, 2) develop a relationship between the system and change agent, 3) define a change problem, 4) set change goals and action plan for achievement, 5) implement the change, 6) staff accept the change, stabilization, 7) redefine the relationship of the change agent with the system [53]. Roger's Diffusion of Innovation Theory, developed in 1962, has introduced following change phases: 1) knowledge, 2) persuasion, 3) decision, 4) implementation, 5) confirmation [53]. And finally, Kotter's Eight-Step Change Model was created in 1995 and included the following steps: 1) create a sense of urgency for change, 2) form a guiding change team, 3) create a vision and plan for change, 4) communicate the change vision and plan with stakeholders, 5) remove change barriers, 6) provide short-term wins, 7) build on the change, 8) make the change stick in the culture [53]. Kotter's model has been identified mostly in nurse-led, local-level, single unit, or site quality improvement projects [58] [54]. As the new standard implementation is a gradual nationwide change and all other change management theories' steps can be categorized under Lewin's three step model (Table 1), the author sees Lewin's change management theory model the most relevant here for analysing the gathered data.

3 Research problem and aim of the study

3.1 Research problem

Ensuring information security and data privacy is critical for all healthcare organisations [9] and although healthcare providers have been trying to implement all mandatory requirements related to information security and data privacy, the acceptance and compliance of those requirements has still been problematic [1] [11].

3.2 Aim of the study

The aim of this study is to identify the viewpoints of different stakeholders regarding information security and data privacy in terms of healthcare service provision in the context of change management.

In order to achieve the aim of the study, author has specified three research questions:

1) What are the experiences of different stakeholders in implementing and complying with information security and data privacy requirements?

2) What are the main supporters of implementing information security and data privacy requirements and changes in the healthcare system?

3) What are the main barriers of implementing information security and data privacy requirements and changes in the healthcare system?

4 Methodology

In this section of the study, author introduces the methodology used. An overview is given of the design, sampling, data collection, data analysis and ethical considerations.

4.1 Study design

This study is a secondary data analysis. The data was firstly gathered for a research project NORDeHEALTH led by Estonia and Nordic countries. According to Estonian Research Information System the project "aims to identify the challenges and opportunities in digitalization of health services" and "increase self-management and transparency in healthcare"[59]. For one particular work package (WP5) the task was to gather information from relevant stakeholders about the information security and data privacy challenges in the ISMS work related to national resident services. NORDeHEALTH partner in Estonia is Tallinn University of Technology (TalTech) under which E-Medicine Centre conducted the interviews with the participants. The same information was gathered and will be gathered from all participating countries to analyse the data privacy and information security situations and issues in all countries (Norway, Sweden, Finland, Estonia).

The primary focus of the project was to gather ISMS related information from the citizen point of view. The author of this study helped to transcribe the gathered data and as the gathered data revealed new topics, the author decided to approach the data from the change management point of view and conduct an independent study with already gathered data. This master thesis focuses only on Estonia and the author's contribution is to analyse secondary data collected from the above mentioned NORDeHEALTH project.

This study is a qualitative research. Qualitative research gathers participants' experiences, perceptions, and their behaviour [60]. One of the strengths of qualitative research is its ability to explain different processes and patterns of human behaviour that can be difficult to quantify [60]. By using qualitative research method, it is possible to see the complete pattern or structure of the participants' insights and understandings [60]. As the aim of

this study is to analyse viewpoints of different stakeholders regarding information security and data privacy in terms of healthcare service provision, qualitative study is the most suitable form of research method as it was needed to gather participants' experiences and perceptions about the topic.

For this study semi-structured interviews with five different stakeholders were performed to gather data. Semi-structured interviews were conducted by the supervisors of this research within the frame of NORDeHEALTH project in Estonia. Semi-structured interviews are becoming increasingly prevalent in healthcare research as they let researchers explore matters in an in-depth mater, allowing insights into how different phenomena of interest are perceived [61]. Semi-structured interviews have an interview guide or prepared questions aimed at addressing the research objective. The questions prepared provide structure and focus on the natural flow of conversation for each unique interview [62]. Semi-structured interview format encourages a two-way communication which creates a comprehensive discussion of the topics [60]. This way there is a possibility to collect more detailed answers rather than generalized understandings of the topics [62]. As the participants of this study are different stakeholders and play different roles in data privacy and information security topics in Estonian healthcare field, it was important to allow the participants to emphasize and guide the topics in the direction that was most relevant to their roles.

4.2 Sampling

For this study participants were contacted and asked to participate by a member of a research staff of the E-Medicine Centre. The participant list was specified by the NORDeHEALTH project manager in Estonia. The participants were contacted through email and asked to participate in the study by explaining the aim of the project and their relevance in it. After receiving the participants' consent, time of the interview was agreed between the participants and the interviewers.

For sample formation the purposive sampling approach was used. Reason for purposive sampling is to better match the sample to the goals and objectives of the research, thus improving the reliability of the data and results [63].

Participants of the study were specified by the NORDeHEALTH project and the request was to conduct interviews with relevant stakeholders on a national and on a regional level. National level represents governmental organisations and regional level represents regional hospitals. Other countries were asked to make interviews with different local governments/regions, but as Estonia was the smallest country and in terms of healthcare local governments are not responsible, it was suggested to interview regional hospitals instead. Participants from national level were specified and chosen according to their roles in healthcare system related to information security and data privacy topics. The sample formation is shown in Table 2.

Table 2. The sample representatives

Institution	Regional/ National	Number of participants
Health and Welfare Information Systems Centre	National	2
Information System Authority	National	1
Data Protection Inspectorate	National	1
Hospital 1	Regional	2
Hospital 2	Regional	3
Total		**9**

The participants on the regional level consisted of 2 hospitals in different Estonian regions. 4 different regional hospitals were contacted, of whom 2 hospitals agreed to participate in the study during the interview months. There are several types of healthcare providers in Estonia, however in this research hospitals represent healthcare providers. Author of this study does not generalize gathered information from hospitals to all healthcare providers and understands that there are many other healthcare providers that are relevant stakeholders in healthcare system. In the results there is a clear distinction whether the opinion is about all healthcare providers given by the governmental organisations, or the opinion comes from regional hospitals.

Organisations on national level had all 1 person participating in the interview. Two separate interviews with the same organisation were conducted as one of them was a test interview. Both regional hospitals had either 2 or 3 persons participating in the interview.

4.3 Data collection

In order to save resources and having some participants in another cities, the interviews were performed via Microsoft Teams. All of the interviews were conducted during the months of September and October 2022. Before the interview started, the participants were introduced of the aim of the study and informed about as well as asked consent to record and save the interviews until the end of the transcription process.

As in hospitals there are several persons responsible for data privacy and information security aspects, all relevant parties according to the organisation were included in the interview. All participating organisations agreed to show themselves visually by using their cameras and be recorded through Microsoft Teams. 2 participants from on hospital interview used only the sound and were not seen through Microsoft Teams. Interviews lasted from 40 minutes to 55 minutes.

Data for the study was collected during the interviews by using two different interview plans (Appendices 1 and 2). The interview consisted of main sub-categories starting from general ISMS process, liability and responsibility, digital health service users, access rights, standards, mobile devices, dangers to patients and future perspectives. The questionnaires for regional and national organisations were slightly different. The main sub-categories were the same, but on national level some additional questions about healthcare sector and new resident services were included. Participants were asked to answer the questions from their point of view that is related to their work in the organisations. Some answers to the questions were further elaborated, while some questions were discussed very briefly depending on the responses and the participants' willingness to talk about the topic. In the end all participants were asked if there was some theme that they would like to bring out themselves or add to the questions already asked.

A test interview was performed before the actual stakeholder's interviews. Test interview allows to check whether the questions prepared are understandable for the interviewees and if the questions lead to the aim of the research [64]. Test interview also gives an

indication on how long the interview might last and allows to also test all technical aspect of conducting the interview [64]. As the test interview was conducted with an employee of one of the stakeholders and data gathered was useful, the test interview was incorporated into the final research sample. The recorded video and audio files were transcribed verbatim using web-based speech recognition programme [65]. Afterwards, the text files were copied to Microsoft Word and were corrected by re-listening the recordings during which missing parts were added and corrections made. Indications on whether answers were given in positive or negative tone (either interviewees were smiling or sighing) were also added. In all the transcriptions the names of the interviewees were changed to the number of the interviewee. Eventually the transcripts were translated from Estonian to English. After transcription process had been ended, all audio and video files were deleted permanently.

4.4 Data analysis

Transcripts passed repeated close reading and secondary data analysis. Thematic textual analysis was performed, and both deductive and inductive coding methods were used for analysing the transcriptions. Thematic analysis is a widely used qualitative analytic method [66] and is used to analyse classifications and present themes that relate to the data [67]. The aim of the thematic analysis is to find the meanings and understandings from the gathered data [68]. The researcher does phrase the aim and the questions of the research, but attention is also paid to the topics that the interviewees themselves have stated to be important [68]. During the data collection, new topics about changing standards and their implementation emerged across all stakeholders.

Thematic analysis provides the opportunity to code and categorise data into themes [67]. Coding is derived from the interviewees' responses, e.g. statements and opinions and it categorises information with the aim of framing it as a theoretical perceptions [67]. A deductive approach to analysing data uses an organising framework comprising of themes for the coding process and is often referred to as a starting list [69]. Initial codes were drawn from interview questions. Figure 1 shows what were the three initial categories for data analysis.

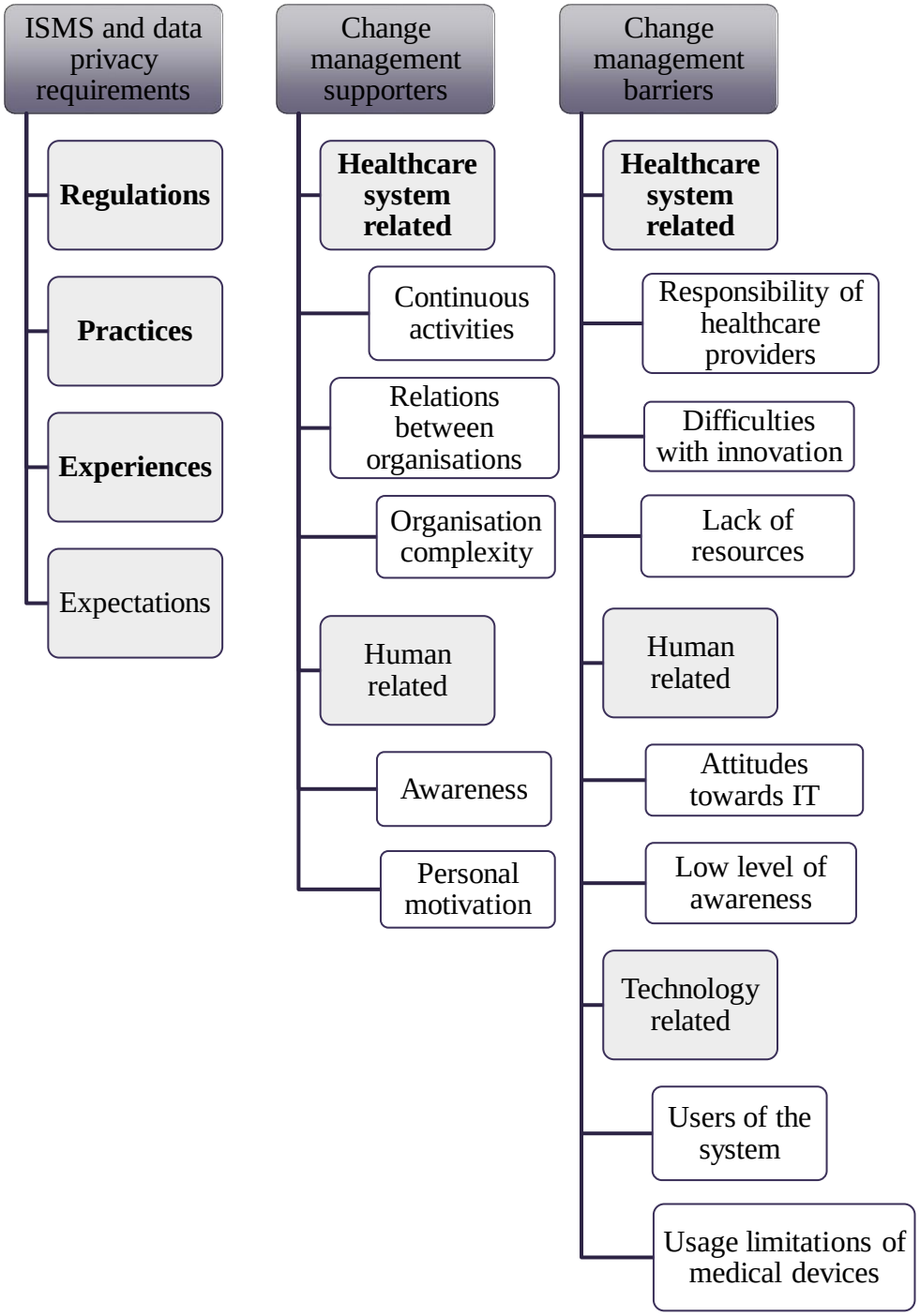

Figure 1. Data themes and coding

After developing cluster of data from the deductive analysis, an inductive analysis was conducted where new codes were created during data analysis phase. Codes generated deductively are marked with bold, other codes were generated inductively. A theme is generated inductively from the gathered data [70]. Inductive analysis moves from more specific observations to broad generalisation, and it allows researcher to generate theory from collected data [71].

4.5 Ethical considerations

The participation in this research was voluntary and participants had a possibility to withdraw from involvement in the research at any given time. During the research no personal data was gathered. As the conducted research was based on expert interviews whose opinions and viewpoints about topics concerning healthcare system were gathered, no approval from Estonian ethics committee was needed.

All of the interviewees were given an overview of the aim of the project before the interview began. The participants were informed about how the gathered data will be used and where the results will be shown in the future. Every participant was also asked for possibility to ask additional questions in written form by email after the interviews. Although each participant agreed to that, the possibility was not used.

All of the gathered data was stored in TalTech OneDrive cloud server, which was protected with a password. The collected data and transcriptions were accessible only to the project team members and the author of this study and was not available to third parties. The audio and the visual recordings were deleted in February, after the transcribing and translation were fully completed. According to the information received from the owner of the web-based speech recognition programme prof. T. Alumäe (private correspondence), the files were stored for 1 month and deleted afterwards. The transcribed interview texts were only shared with the project initiator NORDeHEALTH and will not be presented in any study or on the Internet. Since the research was a part of a larger study, the transcribed texts will be maintained for up to 5 years to allow publication of the project results. For the data analysis in this study only specific ideas or thoughts of the interviewees will be used to present the results. The used thoughts will be presented as quotes.

5 Results

This chapter presents analysed results found from the interviews. Each of the main themes consist of sub-categories about topics that reflect the viewpoints of different stakeholders about information security and data privacy requirements for healthcare providers.

5.1 Information security and data privacy requirements for healthcare providers

This theme analyses what are the general experiences and perceptions of currently used information security requirements in healthcare providers' work. The codes generated for this chapter were regulations, common practices in compliance, experiences and perceptions about requirements and expectations for the future scenarios.

5.1.1 Current information security standards used and their practices

In the beginning of the interviews, participants were asked about their opinion on information security in the organisations. It was mentioned that for the organisation to reach information security, different levels of it need to be understood:

> *"/.../ firstly there are technical solutions like antivirus programmes, different firewalls, other applications. Then second step is the culture of the organisation, rules, order, information security standard, /.../ and then third is what we do here, meaning the person behind this device, this screen and /.../ cyberhygiene, cybereducation." (I-5)*

This quote shows that information security is seen as a very broad topic involving different parts and levels to be approached in order to reach security of the information in the organisation. The participant from the governmental institution mentioned the relevance of the long-term process:

> *"...to reach this security by design there is long way to got but our main control points and basic themes that need to be in place from the information security point of view, these have been nicely done." (I-2)*

This excerpt suggests that there is still a lot to improve in the organisation, although basic security measures have been in place and functioning. Another participant argued that in bigger Estonian hospitals the situation with information security is acceptable but when it comes to small healthcare providers, the compliance is quite low:

"*In smaller healthcare providers, it's not a question about whether there is a person dealing with information security, the questions is whether there is a person who deals with IT at all /.../" (I-5)*

These quotes show that compliance with information security requirements is quite different depending on the organisation and its size and that opinions from different organisation representatives are also diverse. When asked about first thoughts on current information security measures used, many interviewees brought out the current information security system called ISKE. It was claimed that ISKE is quite complicated system to follow and implement and is not an optimal option to reach information security in the organisation:

"Grundschutz [original standard base for ISKE] *is ..., around two-thousand-page long set of rules issued every year, which probably even the writers themselves do not know how to read. It is basically impossible to do it in a more complicated way" (I-6).*

By 2024, current IT security standard ISKE will be replaced by the new Estonian Information Security Standard called E-ITS. This means that healthcare providers need to change their ISMSs so it would comply with the new standard. Healthcare providers shared an opinion that this is a positive change, but has some issues as well:

"/.../now new standard E-ITS is coming, which is a bit more reasonable [standard], */.../ it leaves a lot of freedom to figure things out for the organisation and in some way this E-ITS is /.../ more difficult to be audited against later on. Freedom is oftentimes the hardest issue." (I-3)*

The interviewees agreed that E-ITS describes what must be done but is not describing the way how to achieve it which leaves a lot of room for self-interpretation and often confuses the healthcare providers as *"/.../ with freedom you always think that what I have done, is not enough" (1-4).* These quotes demonstrate that hospitals are positive about new information security standard, but there is some uncertainty with how to implement it and how to be sure that what they have done in their organisation is enough to be compliant with the requirements. It shows that even though healthcare providers comprehend the changes the new standard will create, they still need support with understanding on how some functions will work. Another hospital's perspective revealed understanding the need but not prioritizing it the highest:

"We know that this change is coming,/.../, in a long perspective we have a row of activities that need to be done /.../ but we move with it as much as we can." (I-7)

Here the quote indicates that even though hospital is aware of the change and understands the importance of it, however the topic is not the biggest priority where to allocate their already limited resources. Another interviewee added that the transition brings in some specific changes and details:

> *"We have to get in place many nuances. With self-evaluation we are somewhere around 50% of the expected level, so there is a long way to go." (I-8)*

This quote shows that having many nuances to implement makes it quite complex process from the change management viewpoint. Participants elaborated more on how the new standard will work in the organisations:

> *"The idea of E-ITS is that it is not built up by stages, but the logic of it is actually that it is applicable for all parts of the organisation, that it is not just information technology approach or thinking. Instead, it applies across all the processes, business processes and actions. It's broad-based and continuous… That all business, office, saving of the documents, passing to the third parties,/…/, implementation of continuous process-based way of thinking." (I-7)*

The above quotes describe that there will be some changes that need to be implemented in the hospitals as the compliance currently with the new standard is for one hospital around 50%. Additionally, the transition will have to change the way of thinking in the organisation as the new standard will be a part of every process and activity.

The interviewees from the governmental organisation level mentioned that many organisations are currently struggling with this transition as there are even organisations who do not know that this transition is mandatory for them. There are ongoing trainings for all relevant organisations, but the participations in them is low and they are continuing investing their time and money in auditing against the old standard:

> *"Half of our country is currently in struggle with how to transit to it. Some are even doing /…/ ISKE audits right now. Which considering that we are /…/ going on a new standard is to put it mildly waste of time and money." "Does everybody know that they have to start using this E-ITS? No, they don't! "(I-6)*

This quote shows that even though there are organisations that are preparing themselves for the new standard there are also some healthcare providers who still need to be informed about the upcoming change.

All in all, the participants stated that information security wise there are many improvements to be done, especially in smaller healthcare providers, but main control

points have been implemented meaning that information security has a strong base. As the transition from one information security standard to a new one is an actual topic, participants opened up about the new standard claiming that the transition will be quite big and nuanced change, which will require support, but at the same time the new standard itself was seen as a better way to secure the information in their organisation when compared to the currently valid standard. Although hospitals claim that they need support with this transition, governmental organisations have made steps to smooth the transition, but the process needs some improvements as supposedly the participation in trainings is low and the information about the transition has not reached yet all relevant parties.

5.1.2 Everyday practices and experiences of stakeholders with mandatory requirements and regulations

During the interviews it was claimed that in healthcare information security and data protection are both very important topics and it is important to understand the differences and similarities of them:

> *"/.../if we talk about hospitals, /.../, then information security and data protection need to be handled separately." (I-4)*

Additionally, a hospital representative claimed that they *"are still searching for a decent information security officer"(I-3)* and another participant stated that information security and the upcoming new standard are time and resource consuming and therefore *"/.../information security wise we have found ourselves a partner, who consults us 24/7 in that field" (I-7).* These quotes show that information security requires a specific knowledge and constant work in the organisation.

When it comes to information security and data privacy in hospitals, then according to one participant hospitals are dealing with finding balance between compliance and providing healthcare service to patients:

> *"And it is like a dissonance that from one side the business wants to work 24/7 as easily, operatively, accessibly as possible, /.../, to save the patient's life or see some indicators. And on the other side we push the boundaries with information security and data protection. /.../ we need to always find that balance too, that with all that protection and security we wouldn't start interfering with patient's health. And at times those two aren't very compatible together, as we must accept either health risks or ..., more complicated access." (I-4)*

This quote shows that hospitals feel that in some cases information security and data privacy issues prevent healthcare providers from doing their main work and there are situations where those organisations must make decisions about what risks are more important. Additionally, if compared to small healthcare providers, in big healthcare organisations it is much more complicated to comply with all the requirements as in *"small healthcare providers are things more simple, because the number of people, services, machines, /.../ the variety is much smaller and it's easier to get things under control" (I-4.*

When asked about opinions and viewpoints on data privacy and protection, the issue with people's right to know who and why has accessed their data came up. The issue that was brought out by the participants was how the data in shown for the patient:

> *"Sometimes, /.../, a person makes a query from Patient Portal /.../ and patient sees only general information that the hospital has made a general query without the employee's name. This way person cannot judge if the hospital did have a reason to access his data and leaves him with a question why his data was looked at." (I-5)*

The quote shows that even though patients can see what organisation has accessed their health data, sometimes there is no information on who exactly has looked at that data and/or why. This may leave patients confused as they cannot get the certainty that everything is correct and in compliance with his rights.

In conclusion, it was emphasized that both information security and data privacy and protection require specific knowledge and time and that they should be handled separately. Finding balance between requirements and patient's health was emphasized as a problem hospitals sometimes face in their work. Lastly, regarding data privacy and protection, the topic about displaying data correctly and fully to patients in order not to confuse the patient about his rights.

5.1.3 Experiences regarding the implementation of GDPR

Participants have claimed that the awareness about the GDPR compliance issues and patients' rights have grown and *"patients are very concerned about their data" (I-3)* and that is why their "*data protection unit is actually dealing mainly with privacy and data ownership issues" (I-3).*

Regarding GDPR the participants shared an opinion that during the last four years the regulation has been in force, not much changed for the healthcare providers in their work after regulation:

> *" I would say that this general regulation on data protection did not bring like any big or important changes in regards to data accesses or restrictions." (I-5)*

Even though technically not many changes were needed to be done, there was a shift of change in the way of thinking in the organisation. As GDPR allows to fine organisations for violating the provisions, *"it created this fear of a data protections and fear is a big motivator" (I-6).* This statement also matched with the opinion of the participants of the hospital:

> *" With GDPR came this kind of panic and all sorts of trainings and information that what will happen now and that organisations will be fined 20 million. In practice, that date did not bring any drastic changes or rearrangements. "(I-7)*

These quotes show how the implementation of GDPR regulation, which in healthcare did not require many changes, was probably communicated to healthcare providers in a way that created this panic and fear among those organisations. However, the participant from national level see this grown awareness as a positive aspect as it made healthcare providers control their working mechanisms:

> *"But yes, if this has raised the awareness and thinking in data processors, if everything is correct and maybe they evaluate their processes and services more often, then this is only a good thing." (I-5)*

This sub-chapter showed what were the experiences on GDPR related changes in the organisations. One of the most important aspect that came out was that just before GDPR came into force, there was panic and fear among healthcare providers even though not many changes needed to be implemented in the organisation for complying with the regulation. This means that the change implementation and management process should have been managed in a better way, without creating fear of paying huge fines.

5.1.4 Expectations for the future

Participants from the hospitals brought out that they would like to make the process of accessing data for medical personnel a bit easier and even more interactive:

> *"But for some occasion we want to create this possibility that doctor does not need to go and make a query about whether there are news about the patient, but*

rather we put the data on the doctors table that something has changed /…/. There should be a possibility to see that data without a doctor. (I-4)

A participant from a hospital also elaborated on the topic of data accessing and giving consent by hoping that in the future the giving of the informed consent will be easier:

" It would be very convenient to sign the consent digitally at home. But the law says that the consent has to be informed meaning that actually the doctor or medical personnel should meet the patient and then explain to what the consent is exactly given. But that all takes too much time. So yes, everybody is now thinking how to solve this digitalisation issue. (I-4)

The quote shows that hospital representatives are finding the informed consent necessary, but an inconvenient process for all parties and that the current process is not the most optimal solution. Ideally the whole process without giving in the patient's knowledge and understanding about what he is agreeing to, the informed consent of the patient could be given digitally, but the best solution is yet to be developed for that.

For the future expectations a new topic of more systemic approach and the integration of different systems was mentioned by the participant of the hospital. Healthcare could be seen as a broader system where social coherence would be involved:

"*There has to be social coherence. That healthcare, local government, social help, /…/ in Estonia there is no good framework for that, /…/ how to pass the responsibility or how to say that this social worker has access to specific patient's data and how much does he has to know. (I-4)*

Although the participant did not have a good solution for that, it is hoped that these kinds of discussions will be *"discussed more" (I-4)* meaning that the IT departments of hospitals feel strongly that healthcare is a much more broader field and that many issues could be either prevented or solved by other institutions as well. This kind of expectation for bigger cohesion indicates also the role of consciously planned and implemented change as it would involve many new stakeholders and reallocation of the responsibilities.

To summarize, participants are hoping that in the future the information would be more easily accessed in some situations as that would make the process of treating a patient more optimal for doctors. Some hopes for more digital solutions were expressed where some documentation like informed consent could be done before the appointments. Additionally, opinions about more cohesive treatment environment were brought out as

better communication and integration between different institutions like social care could be more involved.

5.2 Main supporters for implementing and complying with the information security and data privacy requirements

5.2.1 Healthcare system related supporters for compliance

The interviews began mostly with the question about what the participants' first thoughts on information security from their professional point of view were. What was mostly mentioned from the participant of the governmental organisations was that *"/.../ information security has to be a constant process and an everyday activity to ensure it" (I-2).* This indicates that information security in the organisation is not a one-time task but has to be dealt with constantly. Additionally, governmental organisations' technological developments and systems, *"must always meet some certain requirements and the developments pass the information security tests" (I-1*) before going live and their solutions are constantly " *being tested during the period the product is used" (I-2)* to guarantee the information security levels.

The participant from one of the hospitals claimed that trainings were seen as one of the ways to achieve that constant process in their organisations:

> *"It is called lifelong learning, for the last three years or so we have had cybersecurity trainings and they are mandatory for certain level of employees. So only through trainings, here it cannot be done any other way. (I-8)*

The quote indicates that in some healthcare providers mandatory trainings must be conducted so that the know-how would be up to date. Although different trainings have been provided for healthcare providers to educate them on information security and general digital awareness topics, more focus has been also put on different tests:

> *"/.../ tests are being performed in the end of the trainings to understand if this digital awareness or digital security awareness has been grown. (I-2)*

Conducting tests for the same purposes was also mentioned by the participants from the hospital:

> *"We have acquired CybExer's security tests that are common in governmental organisations, it is a three-level test./.../ and there are other organisations that did that too." (I-7)*

What helps additionally hospitals with continuous compliance is a good communication between hospitals and governmental institutions:

> *"One hospital contacts us monthly, sometimes even weekly with one of our specialists and they talk about different topics, sometimes preventively." (I-5)*

It was also claimed that with one specific governmental organisation hospitals *"have tried to find so called weak spots" (I-2)* regarding information security. These quotes show that when the know-how is not strong enough, hospitals turn to governmental institutions for help which gives them then certainty in their decisions and actions. In addition to good communication, there is also trust in governmental organisations and their systems:

> *"This information that we send to Patient Portal, we pack them together and we believe /…/ that the X- road is safe and Patient Portal will keep that data safely. (I-4)*

When asked about the ways how exactly does each healthcare provider take responsibility for their information security measures in their organisations then the viewpoint for that was that smaller healthcare providers like general practitioners will be facing difficulties with the new standard and therefore from the government side it will be facilitated a bit:

> *"Can they manage that responsibility? No they can't! Do they need help? Yes, they do! So there is a pilot project for general practitioners, /…/. This kind of 15 point guide, which says that if you have done these things correctly, you have reached, /…/ 50% of the protection that you would get, if you would do everything correctly." (I-6)*

Additionally, the view is that the systems must be secure, and the governmental institutions try to help to accomplish that as much as they can:

> *"We do whatever we can to achieve that* [security]. *Our aim is not to go and punish. We punish only when we see that nothing else helps and maybe with that one punishment others will also learn." (I-6)*

These quotes indicate that the aim of the governmental institutions is to help organisations to implement the required changes by providing simpler solutions and supporting them. Nevertheless, there can be occasions where ongoing problems or non-compliance might require more drastic measures to reach the aim.

All in all, information security is seen as a constant process, where participants conduct trainings and tests, that are oftentimes mandatory, to ensure that. Good communication and trust between some stakeholders was emphasized, which helps to ensure that the

requirements are being followed when the know-how is not sufficient. Additionally with some healthcare providers, governmental organisations have facilitated some processes for them so the compliance would be reached. Their aim is not punishing the healthcare providers when mistakes or non-compliance occur, but rather help and support those organisations who need assistance.

5.2.2 Human-related supporters for compliance

The interviewees mentioned that for the hospital employees it is important to also motivate them and explain why the knowledge on information security is important. One of the approaches used is to broaden the gained knowledge to everyday life outside of work environment as well:

> "*We introduced this cyber hygiene training from the perspective that the training will benefit them outside of hospital as well to protect their close ones and that did "sell", that raised the participation process higher. (I-8)*

The quote shows that sometimes employees need additional motivation to participate in mandatory trainings and when included their personal benefit as motivation, then the participation rate grew as well.

A participant from the hospital brought out the topic that the employee should not be afraid of the requirements and that *"everyday instruction for the personnel is that the patient's life is most important" (I-4)* while emphasizing that *"we cannot create a formal barrier that an intensive unit doctor cannot access the patient's data because he has not filled out some forms or applications" (I-4).* These quotes show that organisations take care of their employees and if needed, they will try to find solutions to the problems afterwards as the patient's life is always more important than compliance with information security and data privacy requirements.

Different participants pointed out that having a mandatory authentication when accessing different information systems has given a bigger sense of security for using different systems:

> *"This* [authentication] *reduces the pressure a bit that maybe somebody left the computer and the window open and that someone else finds out the password and will use it." (I-3)*

Participants from national level emphasized that the *"authentication methods have been so called secure by design from the start (I-2)* and that has given a better understanding to users and has created in a way a *"basic hygiene, which has to be implemented to any*

kind of organisation as everyone can be under attack" (I-2). This quote indicates that having specific measures in place in different fields contributes to individual behaviour as it is being understood as a normal part of process and therefore is not being questioned.

In conclusion, participants mentioned that in order to maximize the participation in trainings and to keep information up to date, personal motivation has to be present meaning that if an employee gets his personal benefit that he can use outside of working environment, the involvement rate is then higher. Additionally, it was mentioned how organisation will always prioritize patient's health over regulations and requirements if it should come to that point, which supports the medical staff in their job as they feel the support in helping their patients. Having some practices like authentication through all organisations for a long time in place, also helps employees to accept it as a normal part of the process.

5.3 Main barriers for implementing and complying with the information security and data privacy requirements

5.3.1 Healthcare system related barriers for compliance

When asked about the compliance with the national information security standard, then the participant from the regional level stated that there is a lack of resources for controlling every organisation and therefore the responsibility lies on the healthcare provider to ensure that the services they use, are secure as well:

> *"/.../ responsibility is divided from one side to this software producer, who has promised to their clients that it's all good and secure. /.../ and on the other hand, the healthcare provider has confirmed that yes, we use for example ISKE here. And that today somebody would go and control it, no, we do not have these kinds of resources." (I-2)*

The same issue was brought about compliance of data privacy as here healthcare provider is responsible for following all the requirements and restrictions:

> *"If a hospital or a general practitioner has been given a permission to interact with health information system and this hospital or general practitioner uses it somehow unlawfully, in other words uses it not for specific treatment case, then government cannot control it in any way, and it is then the responsibility of that healthcare provider." (I-5)*

These quotes show that organisations cannot control every part of the requirements healthcare providers must follow and they need to trust the healthcare providers. It does not necessarily mean that it is a negative aspect, but it does leave more room for errors and data breaches for healthcare providers. Additionally, the opinion is that these breaches are mostly not intentional and even with this freedom, the data protection minimality principle should be applied:

> *"Well, you can't say that government has created premises for wrongful usage here, they are rather small user mistakes or slip-ups, where healthcare professionals take the easy way out and make this extended inquiry to see patient's data." (I-5)*

This view was elaborated from one of the hospitals regarding data accessing with saying that "*as we are responsible for the data, we have to think very thoroughly whether we trust this application or this third-party platform" (I-4).* Meaning that when a hospital is approached by some third-party for cooperation, the hospital then has some conditions that this third party has to comply with to minimize the risks of having a data breach and oftentimes these conditions do not suit them, and the cooperation is cancelled due to not being able to follow the conditions:

> *"And then we minimize the risk with telling them that in that project patients have to agree to terms, the informed consent must be taken, and /…/, some projects pull the trigger at that point, because they say that it is too complicated to explain to the patient why their data is stored in some cloud." (I-4)*

These issues with Estonian data protection framework and GDPR compliance also are in a way preventing innovation in the healthcare as there are some services that medical personnel would be interested in using or participating in, but due to regulations it is not possible to use them:

> *"We are falling behind in comparison with other continents because we cannot use these services very operatively, /…/, and we have to tell our doctors with sad faces that the law forbids us sending the data there and we cannot use their services. So, this is like a problem, the other world is moving on." (I-4)*

What was also felt that the local interpretations of GDPR are a bit different and sometimes it appears that other European countries can participate or use some service in the same legal framework when Estonia cannot:

> *"Here in Europe these local interpretations of this GDPR tend to be with different kind of harshness level or so. There has been a situation where Germans, who are*

very pedantic, are able to use some specific solution, so why we here in Estonia cannot." (I-4)

These quotes show how hospitals do understand the importance of the information security and data privacy, but also feel that sometimes they prevent medicine from innovation to try or incorporate some new services, which could be useful for medical personnel in their work.

In relation to implementation of both information security and privacy measures, responsible positions like chief information security and data protection officers should be present in the organisations and *"those data protection officers have actually quite a big role and responsibility"* and "*they should be independent positions" (I-5*), but actually *"these tasks are fulfilled in addition to other responsibilities and therefore, those data protection officers are not up to the job" (I-5).* The participant then elaborated that it can lead to some quality issues as *"they do not have enough knowledge or skills, so they make some mistakes" (I-5).* This quote shows and confirms another participant's view that regarding information technology and security *"everything is done within the possibilities" (I-4)* as many things *"have to be done very quickly and optimally" (I-4)*, meaning that hospitals need some improvement in implementing this work systematically and allocate resources more strategically in this area.

To conclude, there was a strong opinion about the responsibility of the healthcare provider, where the healthcare provider is responsible fully for every employee's access and behaviours but also for the compliance of every partner they would like to cooperate with. Governmental organisations do not have the resources to control healthcare providers themselves, although it is not clear if they should. This responsibility makes healthcare providers very cautious for all third parties like some application providers and sometimes the legal requirements prevent them from cooperation and therefore from using innovative solutions. Lack of resources was brought out as a reason why hospitals do not have often the required know-how, which can then lead to quality issues.

5.3.2 Human related barriers for compliance

Participants share an opinion that the weakest link in both information security and data privacy topics is a human and that however strong are the systems and restrictions in the organisation, human errors can and will occur:

"/.../even in the most cybersecure or let's say in the most knowledgeable organisation there is around quarter of people at least who are in this context the weakest link." (I-6)

A participant from a hospital shared this opinion:

"/.../ it has been said that the weak spots of the systems are found, but I think that systems are assured and secured and that the weak link today in our whole chain is actually a human – some kind of user." (I-2)

These quotes indicate that data breaches among medical personnel can occur even in the most secure organisations until there is a human factor represented. This means that this has to be kept in mind in all the ongoing processes and during the change implementation process. Eventually it is also the responsibility of the employee if errors or breaches occur in the organisations.

When talking about responsibility of a patient, a topic concerning data privacy and giving consent by the patient was brought out where *"patients must know to what they are agreeing to" (I-4).* Meaning that healthcare providers need to ask consent from the patient to process and store their data but there is no knowledge about understanding the consent:

"We can ask people how many times this week they have signed somewhere- I have agreed to the,/.../ terms and regulations. Well, nobody ever reads what is written in there. So here the question is that how do we know that the patient was really informed." (I-2)

So, the quote indicates that people and patients might give their consents without understanding to what they are agreeing to which is also a complex issue for healthcare providers as the responsibility to inform the patient lies on them. On governmental level there are currently discussions about whether to allow different applications accessing and sending information to health information system where the basis of it is patient's consent, meaning that if a patient gives consent, the application can access their data. And here especially the consent needs to be informed:

"/.../ if this kind of agreement will come and that the agreement and responsibility is between the person and the producer of the application. /.../ Then well, maybe the government cannot do anything else. And /.../ the responsibility is, /.../ self-taken by this informed consent giver." (I-2)

This view was also backed up by another participant who claimed that *"we cannot protect the part, when a person goes into a public space, opens his laptop and looks at his health data" (I-1)* meaning that eventually that individual can do with his data what he wishes.

These quotes show that if the agreement comes through, the responsibility is then left to the person giving consent. That means that the person himself has to also be sure that the application used is compliant with all requirements and regulations like GDPR for example. An opinion from one participant from governmental organisation was that people are not yet ready to take that full responsibility and that there are a lot of so called "health" applications that actually do not need access to the person's health data:

> *"... for example, does Taro card application need your health data to better predict your death date? I don't know, probably not. /.../ so are we sure that the government has to help people to make stupid mistakes?" (I-2)*

This quote shows that there are different opinions on liberality in Estonia, but the excerpt indicates that allowing people decide who can access their health data themselves is not always the best solution for the patient.

To end this sub-chapter then participants also mentioned attitudes towards information technology. From the participant on the regional level in was referred that there is this kind of opposition or negative attitude that often appears with every aspect that concerns information technology. Here was an excerpt how the small healthcare providers will probably react to the implementation of the new information security standard:

> *"I am sure that from many of them* [healthcare providers] *we will get complaints before even realising that we have already made an exception for them and made so much easier rules for them to follow." (I-6)*

Additionally, the participant claimed that this kind of perception is especially felt in older generation healthcare service providers who often turn to their organisation and ask, *"why do you bully us* [doctors] *with this IT, don't you really have nothing else to do"(I-6).*

These quotes show that even though there are steps from governmental side that try to facilitate the process of the transition to the new standard, there still exist the opinion that healthcare providers will see that and every other change related to IT as a burden which in change management context needs to be strongly taken into account.

To summarize, the opinion was that however strong are the information security measures, the weakest link will always be the human or the employee who is the user of the system. From the patient side there was also an opinion that allowing people fully decide to whom their health data is accessible is not the best solution as oftentimes people do not apprehend fully to what they are agreeing to when it comes to different consents and terms and conditions. Lastly, when it comes to medical staff and information

technology in general, frequent opposition to IT related changes was brought out even though there have been made steps to facilitate the process of some implementations.

5.3.3 Technology related barriers for compliance

The Health Information System is used by all healthcare organisations. Although organisations are not interacting to each other, each of them must comply with information security requirements in order for it to be used safely. The participants from the governmental organisations brought out that having so many accesses to Health Information System might be creating a risk for data breach:

> *"/.../ network, who use health information system, is very broad with dentists, nurses, different kind of institutions. And so, there are many possible vectors for an attack." (I-2).*

While data breaches occur often through an individual, then there might be different kind of data breaches regarding the technology and machinery healthcare providers use. The main problem here is the old systems in the machines:

> *"In terms of information security, we should take down some older medical device, but there is no money to buy new one, /.../, but at the same time the machine is physically working correctly. This kind of situations is when we need to find compromise. (I-4)*

Similar issue with medical devices and machines was brough out from the governmental organisation's side as well:

> *"And it is not allowed to take it* [medical device] *down even for one or two weeks so new protective measures could be installed on the operational systems, because that machine is in use all the time. But what the hospital management does not understand that if you do not do it then it is possible to shut down all the hospital's computers and machines for one month through that one X-ray machines from the 90s." (I-6)*

The two previous quotes show the different ways of thinking or prioritizing between parties who are responsible for patients' health and who are responsible for organisations security on information technology level. Regarding machines then it was mentioned that *"in healthcare there could and should be some kind of one approach about what kind of devices are okay" (I-4)* meaning that this field is "*gray area or unvalidated" (I-4)* and this way there would be less risk for a data breach through medical technology.

All in all, some technology related barriers that were brought out were that many different parties having access to the Health Information System means that the more parties there are involved, the more possibilities there are for a data breach to happen. Data breaches can also occur through medical devices, which is seen as a problem because in hospitals it is difficult to convince relevant parties to take down some machinery for updates or replace them at all as resources are scarce and understanding about the risk of data breach is low.

6 Discussion

This chapter will present a detailed discussion of the gathered results by analysing them in the context of the theories and previous studies presented in the first chapters. Based on discussion, research questions will be answered. Additionally, the main contributions will be presented and limitations of this study will be brought out.

6.1 Viewpoints on information security and data privacy requirements for healthcare providers

The study results revealed that even though the *security by design* is yet to be reached, information security wise there has been quite a lot of work done already by both governmental institutions and hospitals and that there is a strong base for improvements and future developments. Although the participants did not give out any numbers, this finding could be brought out next to an analysis from 2019 based on 1723 European hospitals where 70% of those hospitals failed to implement basic security and privacy measures consistent with their digitalization levels [1]. As participants of this study did not emphasize strongly on considerable problems regarding information security in Estonian hospitals, the author supposes here that the results from the previous study would not correlate to current Estonian situation regarding information security compliance and that Estonian hospitals have secured their information on acceptable level. What currently is a problem and needs resources and a good solution, is a situation with smaller healthcare providers whose compliance and readiness for cooperation is quite low. This means that approaches to different healthcare providers should be very well thought through in order to reach the aim of having good information security measures in place in every healthcare provider.

Participants opened up about the upcoming transition to a new information security standard claiming that the transition will require some specific and nuanced changes which they will need help with. At the same time the new standard itself was seen as a much more understandable and easier to comprehend compared to the current one. From Lewin's change management model this positive attitude towards the new standard could be used in the Unfreezing step for the healthcare personnel [53] as there are already hopes that the new standard will be less complicated, and this understanding could help break

the resistance before starting the change implementation process in the organisation. Although hospital representatives claim that they need support with this transition and governmental organisations have made steps to smooth the transition, the process needs some improvements as supposedly the participation in trainings is at this point low and the information about the transition has not reached all relevant parties yet. This result from Lewin's theory point of view [53] would mean that in some healthcare provider there is not enough understanding that the change is needed and that the resistance before starting those trainings was not broken. In addition, the key element of why the change is needed was not fully clear which was an obstacle for moving forward according to another step in Lewin's theory [54].

Finding balance between requirements and patient's health was indicated as an issue in the healthcare organisation. It was claimed that hospitals need to be providing services constantly, but at the same time everything must be secured and private. Regarding data privacy and protection, the topic about showing information to patients was brought out. As patients are getting more concerned about their data, they want to know that their rights are being honoured. But if the information is not conveyed in a very understandable way, it leaves even more questions for the patient about his rights and it is an issue that should be considered. Even if the process is implemented correctly, it is still important to display information understandably for the patient as studies show that ensuring patient privacy is one of the key elements in building trust in the healthcare professionals and healthcare organisation [8] and without providing the certainty about the compliance for the patient, it does not create the trust in the patient [12].

When it comes to preparing for a change implementation meaning the transition to a new standard, there is a good experience from 2018 where the GDPR was implemented. One of the important aspects that was emphasized was that just before GDPR came into force, due to possible fines there was strong fear and panic in healthcare providers, even though not many changes needed to be implemented in the organisation for complying with the regulation. This means that the change implementation and management process should have been managed in a more thorough way. This result in general just shows how important communication and preparation processes are in the whole change management process [6]. It has been also previously stated that the behaviour of healthcare professionals can greatly impact the success or failure of a change initiative and although

fear can be a good motivator, it is not a sustainable way to start the long-lasting process of change implementation [49].

As some researches claim, different IT implementations in hospital have a very strong influence on the whole organisation and its employees [12]. This means that every digitalisation-based change in the organisation has to be managed well and here it would be also beneficial if the need for that change would come from within the organisation as oftentimes when the change is initiated from outside, the change acceptance is more difficult to reach [48]. From the participants some hopes were expressed that in some situations health data would be more easily accessed for the healthcare staff and hopes for more digital solutions were expressed where some necessary documentation could be done before the appointments. This here could be one of the starting points for the organisation if there is a related change planned as this change and the need would be easily understandable for the many employees.

6.2 Main supporters for implementing and complying with the information security and data privacy requirements

Information security was seen as a constant process, meaning that even though there are specific means implemented, it still needs ongoing processes to ensure that systems are in place and that required parties are involved. For that, according to participants, both level organisations have trainings and various tests that are oftentimes mandatory. Here it is important to note that researches also claim that change is a process, where the implementation and consolidation can take many years, and that individuals may go through different stages as they adapt to the new situations [47] meaning also that this adaptation can be individual and that needs to be take into account for any change implementation. From Lewin's change management theory point of view the third step called Defreezing the change means that the new change needs to be maintained and from this view constant trainings and tests are a positive example of ensuring the knowledge and behaviour that is related to initial change implementation [55].

In the interviews good communication and trust between some stakeholders was highlighted, which helps to ensure that the requirements are being followed when the know-how is not sufficient. Good relations and trust between organisations are here seen as big supporters in change management, because as based on previous research, often

lack of trust is one of the common challenges that is being faced in change management process and it is difficult to start a process of an intervention when there is a lack of mutual trust [49]. Additionally with some healthcare providers, governmental organisations have facilitated some processes for them so the compliance would be reached. Their aim is to help and support those organisations who need assistance which is also a significant supporter for successful change implementation. Although as it appeared, governmental organisations do not have many resources to control every step of the healthcare provider, which means that the help that is given to healthcare providers, has to be evaluated and planned well in order to provide maximum support with existing resources.

Participants mentioned that in order to maximize the participation in trainings and to keep information up to date, personal motivation has to be present meaning that if an employee gets his personal benefit that he can use outside of working environment, the involvement rate is then higher. As data breaches are very prevalent and currently researches that would investigate the factors that contribute to ethical misconduct are lacking [14], it can be useful to use personal benefit as a motivation for employees to comply with the requirements. This approach can be also seen as second step called Moving from Lewin's theory, which promotes the change and where participants try to discover new ways to move towards the desired stage [56].

It was mentioned how healthcare providers will always prioritize patient's health over regulations and requirements if it should come to that point, which in a wider sense supports the medical personnel in their job as they feel the support in helping their patients. Here the whole organisation understands well that patient's life is always a priority and if needed, the solutions will be formed on the go depending on the situation. Participants from the hospital have said that they will not prevent doctors from accessing data in crucial times just because that doctor forgot to confirm something beforehand. This finding correlates well with the understanding that in order to guarantee a successful change implementation, a support from the organisation is needed in all three steps of the Lewin's change management theory, but also in most others change management theories [54]. Without the constant support from the organisation, the employees can feel insecure and might hold back with communicating their concerns [57]. When there is no feedback from the employees, the process of change implementation can be hampered.

This chapter was about argumenting the identified supporters for change management and compliance with necessary requirements. It appeared that there are some activities that already support and make change implementation easier process for relevant parties. Those same supporters are also contributing in being compliant with the existing requirements as they support the behaviour of the initial change and are beneficial for the healthcare professionals.

6.3 Main barriers for implementing and complying with the information security and data privacy requirements

There was a strong opinion about the amount of responsibility of the healthcare provider, where the healthcare provider is fully responsible for all employees' accesses and actions but also for the compliance of every partner they would like to cooperate with. Governmental organisations do not have the resources to control healthcare providers themselves in regard to information security and data privacy, although it is not clear if they actually should. Although there are many automated security measures like authentication and access rights in place that provides security and privacy to some level, this finding indicates that if national authority does not control the compliance of healthcare providers, there is no good overview of what the situation with data breaches and non-compliance in those organisations is. However, good management of patient medical records has to be in place as it protects patients and builds trust in healthcare provider as well as protects physicians and hospitals from claims of negligence [7][2]. Meaning that healthcare providers should be motivated enough without any outer controls to be compliant with all the requirements. It appeared that the responsibility for the compliance has made healthcare providers very cautious of third parties. Due to strict regulations and requirements and not being able to validate the compliance of that third party prevents healthcare providers from cooperation and therefore also from innovation as there have been some application developers whose solutions have been of big interest for the medical personnel. These kinds of situations could be discussed and explained more to the relevant parties in the organisations in order not to create negativity or resistance towards regulations and requirements.

Lack of resources was also brought out several times by the hospitals as in one hospital the transition to a new standard will be led by an outsourced partner as there are not

enough people to manage it in-house. Here it is again possible to draw a comparison line with a Finnish study, which showed that externally initiated change with a top-down processes left employees questioning the new solution [4]. In order to effectively manage change in the organisation, it is important for the healthcare organisations to have a clear understanding of change and to develop a strategy for implementing the necessary changes [47] and although in the future there will be most likely many other externally started changes, the change implementation should be managed internally. Meaning that in this case the changes should be communicated by the person the employees are used to and whom they can trust.

Question about resources was brought out several times. Due to lack of resources positions responsible for both information security and data privacy areas are in some hospitals actually fulfilled as a complementary task by other positions and therefore, quality issues may emerge. This finding could be one of the reasons that may lead to a rise in data security incidents, which in studies has shown to have a growing threat to the whole healthcare industry [5] [6]. By not having the knowledge or resources to train and support the employees in both topics, employees might make more mistakes themselves often without even knowing it. If increasing resources might be difficult in many situations, then in that case resource allocation has to be prioritized. Having quality issues with information security and data privacy in terms of health data which is considered as a personal data of special categories [31] and under the need for greater attention, can have some serious consequences and these are the areas where optimizing is not beneficial for an organisation.

Many participants believed that however strong are the information security measures, the weakest link will always be the human or the employee who is the user of the system and that humans make mistakes and will continue to make them in the future. This finding is confirmed by the different researches which show that physicians are involved in frequent data breach incidents by making very simple mistakes due to lack of knowledge about for example patient confidentiality aspects which can lead to disclosing medical information to other parties [2] [7] [9]. Additionally, people and in this context employees play a critical role in the success or failure of organisational change and is the primary criticality to be managed if a change implementation is planned [47]. This means that this human behaviour needs to be accepted and taken into account in every process and in every change implementation. Previously mentioned researches [2] [7] [9] about human

mistakes then coincide to the finding from this study, where there was an opinion that allowing people fully control to whom their health data is accessible is not the best solution as oftentimes people do not apprehend to what they are agreeing to when it comes to different consents and terms and conditions.

A research shows that there have been multiple concerns from healthcare staff about the impact of digitalization on information overload, interaction with patients, privacy issues, disruptions with workflows and with increasing workflows, which then can contribute to different mistakes [4]. When it comes to healthcare staff and information technology in general, frequent opposition to IT related changes was brought out as an ongoing issue. Even though there have been steps made to facilitate the process of some implementations regarding information security, the participants claimed that it is still difficult to overcome that opposition. From the change management perspective, a study also confirms that for many healthcare employees the implementation of changes in IT and digital innovations is the most disputed area [12]. And that only shows how managing of those fears and reluctance is in a way a so-called project by itself that needs to be managed. By applying here Lewin's change management theory [55], breaking this fear would be the first step before initiating any change. This would be called the Unfreezing step, which in Lewin's theory is strongly emphasized as the resistance needs to be broken before any change implementation [53]. Changes concerning digitalization and including different IT based solutions are only growing [2] which means that in the future this opposition can be a considerable barrier with every change or new implementation if not addressed.

It is claimed that health data is complex, meaning that it resides often in many places, occurs in different formats and is often in unstructured form which makes processing it securely and trusting it quite challenging [20]. This research claim is backed up with the viewpoint of the participants of this study where in addition to previously mentioned aspects, having many different parties having access to the Health Information System means that the more there are different parties, the more there are possibilities for data breaches to take place. In most studies, data breaches are mentioned as unauthorized access to health data or a cybersecurity attack [22], but data breaches can also occur through medical devices, which is seen as a problem for the participants of this study because in hospitals it is difficult to convince relevant parties to take down some machinery to update or replace them at all as resources are scarce and understanding about the risk of possible data breach is low. The opinion of the healthcare personnel is usually

that unless the machines are not broken, they should keep continuing their work. These findings resonate with Peter Drucker's opinion that describes healthcare organisations as two-headed monsters due to having medical and non-medical parties in the same organisation, which can often create conflicts due to different values and understandings [50]. This theory shows how it is important to find the balance and compromise between both parties. In order to take care of the patient physically and at the same have information secured in all aspects in the organisation, effective management of efficient utilisation of the health workforce and of the resources is required [17].

The aim of this chapter was to discuss main barriers for information security and data privacy related compliance and change implementation management. It appeared that participants stated or brought out more barriers than supporters which in a way is understandable as it is usually easier to remember the negative aspects than positives. But it also shows that there are some issues that need to be addressed in order to make information security related change management implementation easier and more amenable for the participants.

6.4 Main contribution

The study contributes to the field of change management in healthcare by offering the insights of different stakeholders in Estonian healthcare regarding information security and data privacy requirements. As there is a starting and ongoing transition from one information standard to a new one, this study gives useful information for the management of this change, but also for other changes related to the implementation of information technology. As various researches claim that data breaches are a very prominent and growing problem in healthcare field, it is very important to have a successful implementation of the new information security standard and to be compliant with all the current requirements and regulations. The study contributes to a smoother transition of the new information security standard by outlining and analysing main supporters and barriers for change implementation and for the compliance of current requirements regarding information security and data privacy. This study has also a relevance in the international context as Estonia has been seen as a pioneer in digital health developments and with successful implementations of these kind of changes,

Estonia can be a good example in the successful implementation of information security and data privacy compliance for other countries as well.

6.5 Limitations

This study has couple of limitations that need to be addressed. Firstly, the sample group was rather small with having only 2 regional hospitals representing the healthcare providers. This means that the results of this study cannot be generalized or standardized to all types of healthcare providers in Estonia. Secondly, this research conveys the viewpoints of different stakeholders, but it does not fully reflect the actual situation and problems in healthcare providers as the opinions given come from different institutions who all specialize in one specific field and can comment on different topics only from their point of view. Thirdly, the viewpoints from hospitals convey the opinions of the IT departments, not the healthcare professionals themselves meaning that hospital viewpoints are filtered through non-medical positions. Lastly, this study was a part of NORDeHEALTH project which had its own pre-defined aims and research questions, meaning that results presented in given study are influenced by NORDeHEALTH overall aims. Although interviewees talked about healthcare provision and compliance in Estonia, NORDeHEALTH project was designed for different countries meaning that it was not a context-specific study, and this could have impacted this study results as well.

Despite those limitations, the author believes that these limitations do not decrease the value of this study in giving initial insights into the topic as it can be used as a strong base for more specific research.

6.6 Future research

As current study conveyed only the viewpoints of two regional hospitals, it would be beneficial to conduct the study with other hospitals as well to get a better overview on information security and data privacy compliance of all Estonian hospitals. As it also appeared from the results that information security compliance in smaller healthcare providers is very low, it is important to address the problem and therefore future research could be aimed at finding the best solutions to engage and support them in order to reach information security in their organisation as needed.

Additionally, the results revealed that governmental organisations do not control additionally healthcare providers in terms of their information security management system nor how are they accessing patients' health data. This indicates that respective authorities do not have a full overview of the compliance level in Estonian healthcare providers. As in the results more barriers than supporters were revealed, it would be useful for future research to go deeper into the reasons why data breaches occur and how they could be avoided. This would contribute to minimizing the negativity to information technology implementations, which then in turn would support finding the best solutions for implementation of information security measures.

6.7 Final conclusions

Based on the findings of this research, following conclusions can be brought out:

1. From the experiences of GDPR implementation and lack of correct communication, better preparation and communication must be prioritized when implementing the new change in order not to create the same kind of fear as previously.
2. Communication and explanations are important aspects in change management process in order not to create negativity and resistance against information security and data privacy requirements as some changes are perceived as inconvenient and limiting innovation.
3. Continuous trainings, good communication between organisations, using personal motivation for employees and organisation's support in situations when it comes to balancing patient's health and compliance contribute to better change implementation and general compliance in the context of information security and data privacy.
4. Lack of resources has been identified as one of the most prevalent barriers and needs to be addressed in a more systematic way both on regional and national levels.
5. Possible data breaches due to human behaviour are very prevalent and as humans will always be the weakest links even with the strongest security measures, human behaviour needs to be accepted and considered in every process and new change implementation.
6. Resistance and opposition of healthcare professionals towards information technology needs to be addressed when it comes to any IT related change implementation. As changes related to digitization are growing, not solving this

resistance to information technology will be a considerable barrier to any change implementation.

7 Summary

The aim of this thesis was to identify the viewpoints of different stakeholders regarding information security and data privacy in terms of healthcare service provision in the context of change management to facilitate the process of change implementation for relevant parties. The author of this study conducted a secondary data analysis by using already gathered data from previously conducted semi-structured interviews with different stakeholders in terms of healthcare service provision. To broaden the change management context, supporters and barriers for change implementation and compliance regarding information security and data privacy were searched and analysed.

The findings revealed that firstly, participants feel mostly positive towards the new information security standard but feel that due to some aspects of it they will need help and support when implementing all the changes in their hospitals. Change management theories with good communication are strongly advisable to make the transition and compliance with the new information security standard much smoother process.

Secondly, there are supporting actions and activities that make change implementation easier process for relevant parties. Constant trainings, good relationships between organisations, organisation supporting their employees, using additional motivation to engage the employees – they all contribute to being compliant with information security and data privacy requirements and with the implementation of a new change.

Lastly, addressing the barriers before change implementation has to be prioritized in the change management process as aspects like lack of resources, opposition to information technology, being fully responsible for compliance, and human behaviour in general which when approached and solved, would facilitate the process of change implementation and also would help to maintain it later on as well.

In conclusion, change management models should be used when implementing any organisational changes in healthcare providers for successful change implementation process. This way people responsible for the change management are better aware about how to approach and solve different problems before the initiation, how to implement that change and how to maintain it later on.

References

[1] S. Uwizeyemungu, P. Poba-Nzaou, and M. Cantinotti, “European hospitals’ transition toward fully electronic-based systems: Do information technology security and privacy practices follow?,” *JMIR Med Inform*, vol. 7, no. 1, Jan. 2019, doi: 10.2196/11211.

[2] N. N. Basil, S. Ambe, C. Ekhator, and E. Fonkem, “Health Records Database and Inherent Security Concerns: A Review of the Literature,” *Cureus*, vol. 14, no. 10, Nov. 2022.

[3] C. S. Kruse, A. Stein, H. Thomas, and H. Kaur, “The use of Electronic Health Records to Support Population Health: A Systematic Review of the Literature,” *J Med Syst*, vol. 42, no. 11, Sep. 2018.

[4] P. Saukkonen *et al.*, “The Interplay of Work, Digital Health Usage, and the Perceived Effects of Digitalization on Physicians’Work: Network Analysis Approach,” *J Med Internet Res*, vol. 24, no. 8, Aug. 2022, doi: 10.2196/38714.

[5] S. Nifakos *et al.*, “Influence of human factors on cyber security within healthcare organisations: A systematic review,” *Sensors*, vol. 21, no. 15. MDPI AG, Aug. 01, 2021. doi: 10.3390/s21155119.

[6] P. Nilsen, I. Seing, C. Ericsson, S. A. Birken, and K. Schildmeijer, “Characteristics of successful changes in health care organizations: an interview study with physicians, registered nurses and assistant nurses,” *BMC Health Serv Res*, vol. 20, no. 1, Feb. 2020, doi: 10.1186/s12913-020-4999-8.

[7] W. Ismail, N. Haayati, M. Alwi, R. Ismail, M. Bahari, and O. Zakaria, “Readiness of Information Security Management Systems (ISMS) Policy on Hospital Staff Using e-Patuh System”.

[8] M. Mocydlarz-Adamcewicz, “Effective communication between hospital staff and patients in compliance with personal data protection regulations,” *Reports of Practical Oncology and Radiotherapy*, vol. 26, no. 6, pp. 833–838, 2021, doi: 10.5603/RPOR.a2021.0138.

[9] R. Karasneh *et al.*, “Physicians’ knowledge, perceptions, and attitudes related to patient confidentiality and data sharing,” *Int J Gen Med*, vol. 14, pp. 721–731, 2021, doi: 10.2147/IJGM.S301800.

[10] C. S. Kruse, B. Smith, H. Vanderlinden, and A. Nealand, “Security Techniques for the Electronic Health Records,” *J Med Syst*, vol. 41, no. 8, Aug. 2017, doi: 10.1007/s10916-017-0778-4.

[11] F. A. Fernandes and G. v Chaltikyan, “Analysis of Legal and Regulatory Frameworks in Digital Health: A Comparison of Guidelines and Approaches in the European Union and United States,” *J Int Soc Telemed eHealth*, vol. 8, Dec. 2020, doi: 10.29086/jisfteh.8.e11.

[12] P. Hospodková, J. Berežná, M. Barták, V. Rogalewicz, L. Severová, and R. Svoboda, “Change management and digital innovations in hospitals of five european countries,” *Healthcare (Switzerland)*, vol. 9, no. 11, Nov. 2021, doi: 10.3390/healthcare9111508.

[13] J. Priisalu and R. Ottis, “Personal control of privacy and data: Estonian experience ,” *Health Technol (Berl)* , vol. 7, no. 4, 2017.

[14] M. J. Yeh and R. B. Saltman, “Creating online personal medical accounts: Recent experience in two developed countries,” *Health Policy Technol*, vol. 8, no. 2, pp. 171–178, Jun. 2019, doi: 10.1016/j.hlpt.2019.05.004.
[15] A. Tsuiman, “Data Protection in Estonia: Overview, Practical Law Country Q&A w-007-4113 Data Protection in Estonia: Overview,” 2020.
[16] “Estonian information security standard (E-ITS),” 2022.
[17] C. A. Figueroa, R. Harrison, A. Chauhan, and L. Meyer, “Priorities and challenges for health leadership and workforce management globally: A rapid review,” *BMC Health Services Research*, vol. 19, no. 1. BioMed Central Ltd., Apr. 24, 2019. doi: 10.1186/s12913-019-4080-7.
[18] H. Ibrahim, X. Liu, N. Zariffa, A. Morris, and A. Denniston, “Health data poverty: an assailable barrier to equitable digital health care,” *Lancet Digit Health* , vol. 3, no. 4, Apr. 2021.
[19] L. H. Yeo and J. Banfield, “Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis,” *Perspect Health Inf Manag*, vol. 19, no. 1, 2022.
[20] H. H. Kim, B. Kim, S. Joo, S.-Y. Shin, S. C. Hyo, and Y. R. Park, “Why Do Data Users Say Health Care Data Are Difficult to Use? A Cross-Sectional Survey Study,” *Journal of Medical Internet Research* , no. e14126, Aug. 2019.
[21] C. Thapa and S. Camtepe, “Precision health data: Requirements, challenges and existing techniques for data security and privacy,” *Computers in Biology and Medicine*, vol. 129. Elsevier Ltd, Feb. 01, 2021. doi: 10.1016/j.compbiomed.2020.104130.
[22] A. H. Seh *et al.*, “Healthcare data breaches: Insights and implications,” *Healthcare (Switzerland)*, vol. 8, no. 2. MDPI AG, Jun. 01, 2020. doi: 10.3390/healthcare8020133.
[23] I. Meriah and L. ben A. Rabai, “Comparative Study of Ontologies Based ISO 27000 Series Security Standards,” *Procedia Comput Sci*, vol. 160, 2019.
[24] M. Mirtsch, K. Blind, C. Koch, and G. Dudek, “Information security management in ICT and non-ICT sector companies: A preventive innovation perspective,” *Computers & Security* , vol. 109, no. 102383, 2021.
[25] M. Podrecca, G. Culot, G. Nassimbeni, and M. Sartor, “Information security and value creation: The performance implications of ISO/IEC 27001,” *Comput Ind*, vol. 142, no. 103744, Nov. 2022.
[26] C. J. Hoofnagle, B. van der Sloot, and F. Z. Borgesius, “The European Union general data protection regulation: what it is and what it means ,” *Information & Communications Technology Law*, vol. 28, no. 1, 2019.
[27] R. A. Tariq and P. B. Hackert, *Patient Confidentiality*. Treasure Island (FL) : StatPearls Publishing , 2023.
[28] J. Shahid, R. Ahmad, A. K. Kiani, T. Ahmad, S. Saeed, and A. M. Almuhaideb, “Data Protection and Privacy of the Internet of Healthcare Things (IoHTs),” *Applied Sciences (Switzerland)*, vol. 12, no. 4. MDPI, Feb. 01, 2022. doi: 10.3390/app12041927.
[29] B. Yuan and J. Li, “The policy effect of the general data protection regulation (GDPR) on the digital public health sector in the european union: An empirical investigation,” *Int J Environ Res Public Health*, vol. 16, no. 6, Mar. 2019, doi: 10.3390/ijerph16061070.
[30] D. Georgiou and C. Lambrinoudakis, “Compatibility of a security policy for a cloud-based healthcare system with the eu general data protection regulation

(Gdpr)," *Information (Switzerland)*, vol. 11, no. 12, pp. 1–19, Dec. 2020, doi: 10.3390/info11120586.
[31] J. Wainer, C. J. R. Campos, U. Salinas, and D. Sigulem, "Open Access Security Requirements for a Lifelong Electronic Health Record System: An Opinion," 2008.
[32] N. B. Henrikson *et al.*, "What guidance does HIPAA offer to providers considering familial risk notification and cascade genetic testing?," *J Law Biosci*, vol. 7, no. 1, Jan. 2020, doi: 10.1093/jlb/lsaa071.
[33] P. Mulgund, B. P. Mulgund, R. Sharman, and R. Singh, "The implications of the California Consumer Privacy Act (CCPA) on healthcare organizations: Lessons learned from early compliance experiences," *Health Policy Technol*, vol. 10, no. 3, Sep. 2021, doi: 10.1016/j.hlpt.2021.100543.
[34] E. M. Lotman and M. Viigimaa, "Digital Health in Cardiology: The Estonian Perspective," *Cardiology (Switzerland)*, vol. 145, no. 1. S. Karger AG, pp. 21–26, Jan. 01, 2020. doi: 10.1159/000504564.
[35] J. Metsallik, P. Ross, D. Draheim, and G. Piho, "Ten Years of the e-Health System in Estonia." [Online]. Available: https://e-estonia.com/
[36] T. Habicht, M. Reinap, K. Kasekamp, R. Sikkut, L. A. Ewout, and V. Ginneken, "Health Systems in Transition Estonia Health system review," vol. 20, no. 1, 2018, [Online]. Available: www.healthobservatory.eu
[37] "The Development of the Estonian Health System Performance Assessment ," 2022.
[38] J. Keen *et al.*, "The effects of interoperable information technology networks on patient safety: a realist synthesis," *Health Services and Delivery Research*, vol. 8, no. 40, pp. 1–162, Oct. 2020, doi: 10.3310/hsdr08400.
[39] P. Kivimäki, "Protecting Data at Resti in X-Road 7," *Nordic Institute for Interoperability Solutions*, Oct. 2021.
[40] ©ryl Jensen, "Digital Health Systems A comparison between Estonia and New Zealand," 2020.
[41] *Võlaõigusseadus*. Accessed: Feb. 11, 2023. [Online]. Available: https://www.riigiteataja.ee/akt/961235
[42] *Personal Data Protection Act*. Accessed: Feb. 12, 2023. [Online]. Available: https://www.riigiteataja.ee/en/eli/523012019001/consolide
[43] BNS, "Riigikogu adopts Personal Data Protection Act," *Eesti Rahvusringhääling*, 2018.
[44] "IT baseline security system ISKE ," *Republic of Estonia Information System Authority* . https://www.ria.ee/en/cyber-security/management-state-information-security-measures/it-baseline-security-system-iske (accessed Feb. 12, 2023).
[45] "INFORMATION SECURITY MANAGEMENT SYSTEM. REQUIREMENTS," *Riigi Infosüsteemi Amet*, 2022. https://eits.ria.ee/et/avalehe-menueue/eits-v2022-en/ (accessed Mar. 18, 2023).
[46] G. Erlingsdottir, A. Ersson, J. Borell, and C. Rydenfält, "Driving for successful change processes in healthcare by putting staff at the wheel," *J Health Organ Manag*, vol. 32, no. 1, pp. 69–84, Mar. 2018, doi: 10.1108/JHOM-02-2017-0027.
[47] F. Milella, E. A. Minelli, F. Strozzi, and D. Croce, "Change and innovation in healthcare: Findings from literature," *ClinicoEconomics and Outcomes Research*, vol. 13, pp. 395–408, 2021, doi: 10.2147/CEOR.S301169.
[48] G. Dagliana, S. Albolino, Z. Mulissa, J. Davy, and A. Todd, "From Theory to Real-World Integration: Implementation Science and Beyond," in *Textbook of*

Patient Safety and Clinical Risk Management, Springer International Publishing, 2021, pp. 143–157. doi: 10.1007/978-3-030-59403-9_12.
[49] A. Yazdani and R. Wells, “Barriers for implementation of successful change to prevent musculoskeletal disorders and how to systematically address them ,” *Appl Ergon*, vol. 73, 2018.
[50] P. F. Drucker, *Managing in turbulent times*. Oxford: Butterworth Heinemann, 1993.
[51] S. Cinaroglu, “Complexity in healthcare management: Why does Drucker describe healthcare organizations as a double-headed monster?,” *Int J Healthc Manag*, vol. 9, no. 1, pp. 11–17, Jan. 2016, doi: 10.1179/2047971915Y.0000000016.
[52] B. Burnes, “Kurt Lewin and complexity theories: back to the future?,” *Journal of Change Management* , vol. 4, no. 4, 2004.
[53] Barrow JM, Annamaraju P, and Toney-Butler TJ, *Change Management*. Treasure Island (FL): StatPearls Publishing, 2022.
[54] R. Harrison *et al.*, “Where do models for change management, improvement and implementation meet? A systematic review of the applications of change management models in healthcare,” *Journal of Healthcare Leadership*, vol. 13. Dove Medical Press Ltd, pp. 85–108, 2021. doi: 10.2147/JHL.S289176.
[55] B. Burnes and D. Bargal, “Kurt Lewin: 70 Years on,” *Journal of Change Management*, vol. 17, no. 2, pp. 91–100, Apr. 2017, doi: 10.1080/14697017.2017.1299371.
[56] I. Bose and S. Gupta, “Change Management Theories: A Study on COMAIR, South Africa,” *Indian J Ind Relat*, vol. 56, no. 3, 2021.
[57] S. T. Hussain, S. Lei, T. Akram, M. J. Haider, S. H. Hussain, and M. Ali, “Kurt Lewin’s change model: A critical review of the role of leadership and employee involvement in organizational change ,” *Journal of Innovation & Knowledge*, vol. 3, no. 3, 2018.
[58] E. Karimi, Z. Sohrabi, and M. M. Aalaa, “Change Management in Medical Contexts, especially in Medical Educa-tion: A Systematized Review,” *J Adv Med Educ Prof*, vol. 10, no. 4, pp. 219–227, 2017, doi: 10.30476/JAMP.2022.96519.1704.
[59] “Nordic eHealth for Patients: Benchmarking and Developing for the Future,” *Eesti Teadusinfosüsteem*. https://www.etis.ee/Portal/Projects/Display/5603e973-0ce6-4b83-87dc-0b5fa845b1e8 (accessed Mar. 08, 2023).
[60] S. Tenny, J. M. Brannan, and G. D. Brannan, *Qualitative Study*. Treasure Island (FL): StatPearls Publishing, 2022.
[61] C. McGrath, P. J. Palmgren, and M. Liljedahl, “Twelve tips for conducting qualitative research interviews,” *Med Teach*, vol. 41, no. 9, pp. 1002–1006, 2019, doi: 10.1080/0142159X.2018.1497149.
[62] O. A. Adeoye-Olatunde and N. L. Olenik, “Research and scholarly methods: Semi-structured interviews,” *JACCP Journal of the American College of Clinical Pharmacy*, vol. 4, no. 10, pp. 1358–1367, Oct. 2021, doi: 10.1002/jac5.1441.
[63] S. Campbell, M. Greenwood, S. Prior, T. Shearer, and K. Walkem, “Purposive sampling: complex or simple! Research case examples,” *J Res Nurs*, vol. 25, no. 8, Dec. 2020.
[64] “Intervjuu kavandamine ja läbiviimine,” *Tallinna Ülikool*. https://www.tlu.ee/~sirvir/Intervjuu_vaatlus_ja_sisuanals/intervjuu_kavandamine_ja_lbiviimine.html (accessed Feb. 19, 2023).

[65] A. Olev and T. Alumäe, “Estonian Speech Recognition and Transcription Editing Service,” *Baltic HTL 2022*. http://bark.phon.ioc.ee/webtrans/ (accessed Feb. 20, 2023).
[66] V. Braun and V. Clarke, “Using thematic analysis in psychology,” *Qual Res Psychol*, vol. 3, no. 2, pp. 77–101, 2006, doi: 10.1191/1478088706qp063oa.
[67] M. Ibrahim, “THEMATIC ANALYSIS: A CRITICAL REVIEW OF ITS PROCESS AND EVALUATION,” 2012.
[68] D. Ezzy, *Qualitative Analysis: Practice and Innovation.* . London: Routledge, 2002. doi: 10.4324/9781315015484.
[69] T. Azungah, “Qualitative research: deductive and inductive approaches to data analysis,” *Qualitative Research Journal*, vol. 18, no. 4, 2018.
[70] V. Braun and V. Clarke, “Using thematic analysis in psychology,” *Qual Res Psychol*, vol. 3, no. 2, pp. 77–101, 2006.
[71] M. Williams and T. Moser, “The Art of Coding and Thematic Exploration in Qualitative Research,” 2019.

Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I, Ieva Marija Kuzminaite

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis A qualitative approach on the viewpoints of different stakeholders regarding information security and data privacy in terms of healthcare service provision, supervised by Hedvig Soone and Kadi Lubi.
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

08.05.2023

1 The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

Appendix 2 - Interview Plan. Interview questions for regional level

The Information Security Management system (ISMS) process

- In your opinion, how far has your organization come in terms of the systematic work with information security and data protection?
- Which steps in the systematic work have been most challenging?
- What would have further facilitated the process?
- …
- How does your systematic work with information security/data protection include eHealth Services for citizens, such as Digilugu etc.?
- If new eHealth Services for citizens will be added, how does this affect your systematic work with information security/data protection?
- In your opinion, what are the biggest challenges regarding eHealth Services for citizens concerning your work with infosec and data protection?
- What methods and tools are used in your systematic work in general?
- In what way are they sufficient?
- What may need to be improved?
- Do your methods and tools (if used) also cover the requirements for information security and data protection regarding eHealth Services for citizens, such as Digilugu, …, or what is required further?
- How did the introduction of the GDPR affect the systematic information security work in general?

Responsibility

- In your opinion, who is responsible for ensuring that information security/data protection is handled in a satisfactory manner regarding eHealth Services for citizens such as Digilugu etc?

The users

- What are the challenges regarding users' knowledge of information security/data protection concerning the use of eHealth Services for citizens?
- What is your experience of consent challenges?

- When is it needed, and when is it relatively reasonable not to ask for consent?
- What are the challenges with users' behaviour concerning the use of eHealth Services for citizens to maintain information security/data protection?
- How can these challenges be met?

Access/authorization

- How are conflicts between authorization needs and maintaining data protection/patient privacy concerning eHealth Services for citizens managed?
- Is it a conflict? Why/Why not?
- Who is responsible for ensuring that the authorizations are appropriate concerning eHealth Services for citizens?
- Who is responsible for checking that the authorizations are managed correctly concerning eHealth Services for citizens?

Standards

1) ISO27000-family – Information Security Management Systems
- Do you use these standards, and in what way do they facilitate or complicate your systematic information security work?
- What needs to be improved?
2) ISO 27799 - Information security management in health using ISO/IEC 27002
- Do you use this standard, and in what way does it facilitate or complicate your systematic information security work?
- What needs to be improved?
3) ISO 27701 - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines
- Do you use this standard, and how does it facilitate or complicate your information retrieval and data protection work?
- What needs to be improved?

Mobile devices

- What challenges do you see with your systematic information security work with the increase in mobile devices?
- How do these mobile devices affect infosec and data protection management?

Threats

- In your opinion, what are the main threats to eHealth Services for citizens?
- How does it affect your systematic information security/data protection work?

The future

- How do you see the future and new implementations of eHealth Services for citizens?
- How is the systematic work with information security and data protection affected by new additional services?
- How can improved methods and tools support you in your work with information security and data protection?
- What is required of the methods and tools to have an effect?

Appendix 3 – Interview Plan. Interview questions for national level

The Information Security Management system (ISMS) process

- In your opinion, how far has the healthcare sector come in terms of the systematic work with information security and data protection?
- Which steps in the systematic work have been most challenging?
- What would have further facilitated the process?
- …
- In your opinion, how does the systematic work with information security/data protection include eHealth Services for citizens, such as Omakanta/Journalen etc.?
- Is there a process concerning the information security work if new resident services are to be added?
- In your opinion, what are the biggest challenges regarding eHealth Services for citizens concerning the work with infosec and data protection?
- What methods and tools are used in healthcare regarding systematic work with information security and data protection in general?
- In what way are they sufficient?
- Based on your experiences, what may need to be improved?
- Do these methods and tools (if used) also cover the requirements for information security and data protection regarding eHealth Services for citizens, such as Omakanta, …, or what is required further?
- How did the introduction of the GDPR affect the systematic information security work in health care?

Responsibility

- In your opinion, who is responsible for ensuring that information security/data protection is handled in a satisfactory manner regarding eHealth Services for citizens such as the Omakanta, x, x?

- What is further required from a responsibility perspective at national level to achieve effective and efficient information security / data protection with eHealth services for citizens included?

The users

- What are the challenges regarding users' knowledge of information security/data protection concerning the use of eHealth Services for citizens?
- What is your experience of consent challenges?
- When is it needed, and when is it relatively reasonable not to ask for consent?
- What are the challenges with users' behaviour concerning the use of eHealth Services for citizens to maintain information security/data protection?
- How can these challenges be met?

Standards

- What is your view regarding the work with current standards in the field?

1) SO/IEC 27000-family – Information Security Management Systems

- Does the healthcare sector use these standards, and in what way do standards facilitate or complicate the systematic information security work in healthcare?
- What needs to be improved?

2) ISO/IEC 27799 - Information security management in health using ISO/IEC 27002

- Does the healthcare sector use this standard, and in what way does it facilitate or complicate the systematic work with information security work?
- What needs to be improved?

3) ISO/IEC 27701 - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

- Does the healthcare sector use this standard, and how does it facilitate or complicate the information security and data protection work?
- What needs to be improved?

Others

- What challenges do you see with the systematic information security work with the increase in mobile devices?
- In your opinion, what are the main threats to eHealth Services for citizens?
- In your opinion, how can these threats be taken care of in the systematic work with information security/data protection?
- How do you see the future and new implementations of eHealth Services for citizens?
- In what way can the systematic work with information security and data protection be complemented to include new services?
- How will new technologies affect the systematic work with information security and data protection in healthcare?
- How can improved methods and tools support the work with information security and data protection?
- What is required of the methods and tools to have an effect?