How the General Data Protection Regulation affects Health Information System innovation:

An explorative study of General Data Protection Regulation challenges and benefits for Health Information System innovation initiatives

Fredrik Christensen
Per Sigve Næss

SUPERVISORS

Polyxeni Vasilakopoulou
Margunn Aanestad

University of Agder, Spring 2020
Faculty of Social Sciences
Department of Information Systems

Preface

This master's thesis is submitted to fulfil the requirements of the degree of Master of Science (M. Sc.) in Information Systems (IS) at the University of Agder, Norway.

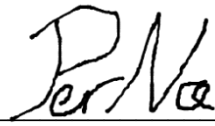
The thesis is conducted based on our interest in the field of IS and IS research, and is motivated by the need for more studies related to the effect of privacy regulations on IS innovation. We are motivated by the possibility to contribute to research in the information systems domain, where information systems are the backbone for further digitalization and technological advancement.

Working on this thesis has enriched our knowledge of IS. We have learned much about IS as a research field, the healthcare sector, and how privacy regulations may impact innovation processes for information systems. The learning curve has been steep; diving into the field of healthcare and privacy regulation regarding information system innovation has been both interesting and educational.

The outbreak of the Covid-19 pandemic was an impediment for this study which was conducted in Norway during the period when the Norwegian government introduced many restrictions to meet the challenges presented by the pandemic. However, with good collaboration, positive and interested participants, as well as good guidance from our supervisors, we have overcome these challenges without any major setbacks for our thesis.

We would like to thank all the participants who agreed to be a part of this study through interviews. We would also like to extend our thanks to our supervisors, who have, through this long process, given the necessary constructive feedback that is vital to ensure the quality of our thesis. Finally, we would like to thank David for all the help with language review.

Fredrik Christensen, 02.06.2020



Per Sigve Næss, 02.06.2020

Abstract

There is a growing demand for health information systems (HIS) innovation to address the challenges of delivering better quality and more efficient healthcare. At the same time, innovations must adhere to increasingly strict privacy regulations especially related to personal health data. While prior research has indicated that privacy regulation can have both constraining and stimulating effects on innovation in general, there is a knowledge gap on how privacy regulation affects HIS innovation specifically. In this master thesis, we study the effects the General Data Protection Regulation (GDPR) have on HIS innovation, and the responses of the health sector and HIS providers. To this aim, we conducted a qualitative explorative study with semi-structured interviews in the Norwegian healthcare sector including both healthcare service providers and HIS suppliers. Our results show that while there is an emphasis on innovating with regulation-compliant HIS amongst the market actors, there are different interpretations of the regulation and different levels of regulation enforcement, affecting cooperation, trust and innovation adoption for HIS initiatives. We furthermore identify that the GDPR is experienced as complicated and not technology-specific when it comes to emerging technologies within healthcare, such as public cloud solutions implemented in Norway for HIS and artificial intelligence and machine learning solutions. This negatively affects HIS innovation building upon these technology paths. We argue that raising the knowledge on GDPR, aligning regulation interpretation and introducing standards can strengthen HIS innovation and aid HIS suppliers to build trust with the healthcare providers. Future longitudinal research is needed to investigate the effects of GDPR on HIS innovation in the long-term, as well as how standardisation of privacy regulation can affect HIS innovation

Table of contents

List of Tables

List of Figures

Abbreviations

AI - Artificial Intelligence
ANN - Artificial Neural Network
CDSS - Clinical Decision Support Systems
DPIA - Data Protection Impact Assessment
EEA - European Economic Area
EFTA - European Free Trade Association
eHealth Electronic Health
EHR - Electronic Health Record
EMR - Electronic Medical Record
ERP - Enterprise Resource Planning
EU - European Union
GDPR - General Data Protection Regulation
GSM - Global System for Mobile Communication
HIS - Health Information System
HIT - Health Information Technology
NSD - Norwegian Center for Research Data
IS - Information System
IoT - Internet of Things
IT - Information technology
ICT - Information and Communication Technology
ML - Machine Learning
OECD - Organisation for Economic Cooperation and Development
ROS - Risk and vulnerability analysis (*Risiko- Og Sårbarhetsanalyse*)
RPM - Remote Patient Monitoring
SCR - Summary Care Record
STS - Sociotechnical System

Terminologies

AI Artificial Intelligence: *"is the concept used to describe computer systems that are able to learn from their own experiences and solve complex problems in different situations- abilities we previously thought were unique to mankind. And it is data, in many cases personal data, that fuels these systems, enabling them to learn and become intelligent"* (Datatilsynet, 2018, p. 4)

eHealth Electronic health: is the use of ICT to provide better healthcare, with systems and technology that aids the processes within healthcare, providing storage, processing, information presentation and communication to the actors involved (Swinkels et al., 2018).

EHR Electronic Health Record: "*EHR is a digital version of a patient's paper chart. EHR's are realtime, patient-centred records that make information available instantly and securely for authorized users"* (HealthIT.gov, 2020a).

EMR Electronic Medical Record: "*Operates the same way as an EHR, but are more focused on clinical data. EMR contains note and information collected by and for the clinicians"*(HealthIT.gov, 2020b).

ERP Enterprise Resource Planning: "*ERP is highly complex information systems. Enables seamless integration of all information flows in the company – financially and accounting information, human resource information, supply chain information, and customer information* (Umble, Haft & Umble, 2003).

HIS Health information systems: "*HIS assist healthcare organisations to gather, process, and disseminate information within the organisation and their environment. HIS incorporates a range of different types of systems, which include patient information systems, administrative systems, radiology and pharmacy information systems, telemedicine and hospital information systems, such as computerized physician entry systems.*" (Sligo et al., 2017, p. 87)

HIT Health Information Technology: describes healthcare combined with technology (Sligo et al., 2017, p. 87)

ICT Information Communication Technology: *Often used as an acronym for IT or an extension to the IT concept. The concept of ICT covers communication technology, computer technology, and assistive technologies related to both"*. (Yang, 2019, p. 205).

IS Information System: *"a set of interrelated components that collect (or retrieve), process, store, and distribute information to support decision making and control in an organisation."* (Laudon & Laudon, 2016, p. 48).

IT Information Technology: "*A technology that is focused around encoding, decoding, as well as the processing of information* (Yang, 2019, p. 205).

ML Machine Learning: *"a set of techniques and tools that allow computers to 'think' by creating mathematical algorithms based on accumulated data"* (Datatilsynet, 2018, p. 5).

STS Socio-technical System: STS perspective is often used to describe and understand the complex combination of information systems and technology, organisations, and people. STS sees an organisation as a combination of technical and social parts combined, and this combination is affected by the environment (Appelbaum, 1997, p. 452-461).

Telehealth: Telehealth is similar to telemedicine, but a broader term, including administration and education (Sligo et al., 2017, p. 87).

Telemedicine: is used to describe the health services delivered to patients remotely (Sligo et al., 2017, p. 87).

1. Introduction

This study seeks to explore the effects that the General Data Protection Regulation (GDPR) has had on Health Information Systems (HIS) innovation in the health sector and what responses organisations apply to meet constraints set by the GDPR. Empirical data were collected through semi-structured interviews with public and private organisations in the Norwegian health sector. The organisations utilise and develop HIS for the health sector, with roles as data controllers and data processors.

The following presents the problem statement, aims and objectives and a synopsis of the thesis.

1.1 Background and Context

Healthcare organisations are faced with pressure related to epidemiological and demographic changes, and there are expectations by healthcare providers, consumers and governments that technology innovation will help address these challenges. HIS can increase efficiency and reduce health expenditure, but HIS innovation and implementation often result in failure. Although electronic health record (EHR) adoption is high, there is limited adoption of information exchange systems, and wider adoption of such systems is sorely needed (Sligo, Gauld, Roberts & Villa, 2017, p. 86-89).

Amongst a number of factors that can impact innovation initiatives, regulation and legislation have a tremendous impact. Regulation can result in market uncertainty, both driving and slowing down innovation, and cause high use of resources when implementing innovative solutions (Blind, Petersen & Riillo, 2017). Storing, processing and sharing of private information are regulated among several countries in Europe under the General Data Protection Regulation (GDPR). The use of personal data can conflict with employees' and consumers' expectations of privacy protection, and the perception of privacy and content of privacy law varies between countries. The GDPR was an answer to further unify privacy law across Europe and introduce stricter criteria for what counts as user consent, higher fines for non-compliance and an expanded definition of personal data (Martin, Matt, Niebel & Blind, 2019).

There is limited research on how the GDPR affects innovation, although some studies have been conducted, e.g. Martin et al (2019). The GDPR has been seen to have both innovation-stimulating and innovation-constraining effects. Personal data has a central role in business models today, and thus entrepreneurs, regulators, public bodies and scholars require an understanding of how the regulation affects innovation, to get an insight in how privacy regulation affect specific domains and the challenges and benefits such regulation impose (Martin et al., 2019). There is limited research and a knowledge gap on how the GDPR has affected HIS innovation, and more knowledge in this domain would lead to a better understanding of the effects of privacy regulation in the healthcare sector and on HIS innovation.

1.2 Problem statement

There is a need for HIS innovation within healthcare, especially where organisations face societal challenges that can be overcome by continuous innovation, but many innovation projects fail (Sligo et al., 2017; OECD, 2017). Innovation is further affected by regulations and standardisation (Blind et al., 2017), and the GDPR as a recent regulation implemented across Europe sets constraints on the collection, storing, processing and sharing of private data (Regulation (EU) 2016/679, 2016). The GDPR may have both positive and negative effects on innovation (Martin et al., 2019), and it is recommended by the OECD to study and examine regulatory frameworks within healthcare, legislation and standards that may facilitate solutions to tackle societal change (OECD, 2017). Therefore, we have conducted an exploratory study to investigate the relationship of GDPR with HIS innovation. The aim of the study is to identify positive and negative effects of GDPR on HIS innovation, and to study how the participants from different private and public organisations have responded to the provisions of GDPR, and what measures are being taken to innovate through regulation-compliant HIS innovation. Based on the findings, we reflect on the effects the GDPR has on HIS innovation, and the responses of organisations linking this study to relevant research.

1.3 Research questions

The purpose of this study is to investigate the effects the GDPR on HIS innovation, and the responses of the health sector and IS providers. Two research questions have been developed towards this purpose:

(1) *How does the General Data Protection Regulation affect health information system innovation for personal health information sharing initiatives?*

(2) *What concrete responses do companies apply to health information system initiatives to meet constraints set by the General Data Protection Regulation?*

1.4 Research approach

This research applies an interpretive exploratory interview-based study design to investigate the phenomena under assessment. The techniques utilised for data collection were semi-structured interviews, with a semi-structured interview guide as the basic structure of the interviews (See appendix A: Interview Guide). We analyse the data through thematic analysis with a deductive approach based on Oates (2006) framework for thematic analysis. For our theoretical lens, we apply Blind, Petersen & Riillo (2017) model of regulation and standardisation impact on innovation in combination with Martin et al. (2019) conceptual framework. We focus on the concepts of strict and lax regulatory enforcement of Martin et al. (2019), applied to the health sector, investigating the enforcement level of the GDPR in the health sector and the further effects the enforcement generates.

Data collections for this study have been performed in eight organisations. Specifically, we got information from nine informants through 11 interviews in Norway. While the GDPR is relevant and impacting the health sector as a whole, this study has focused on HIS innovation, with interviews with public and private organisations located mainly in the South-East and middle of Norway. As this is a master thesis, the time period of the thesis is constrained by the requirements of the master's degree program, one full semester. Thus, the scope and number of informants are set to fit with the limited time given to conduct this master thesis study.

1.5 Personal motivation

Through our participation in the Information System master programme, we have seen how utilization of information systems have transformed different types of industries. In addition, we have understood what challenges a rapidly advancing technology, and digitalization poses on organisations in various industries. Healthcare is one of the industries that have achieved significant technological advancements throughout the last century and is an industry that affects the whole population. Digitalisation and technological advancement also bring challenges connected to privacy and information security.

Having an interest in both technological trends and information security, we were motivated to investigate how the health industry interprets and solves the new challenges that arise when implementing GDPR. Furthermore, we are motivated to contribute to the Information Systems research field by revealing how novel health innovations are affected by the new regulation.

1.6 Thesis structure

The overall structure of this thesis is summarised in the flow diagram of Figure 1.

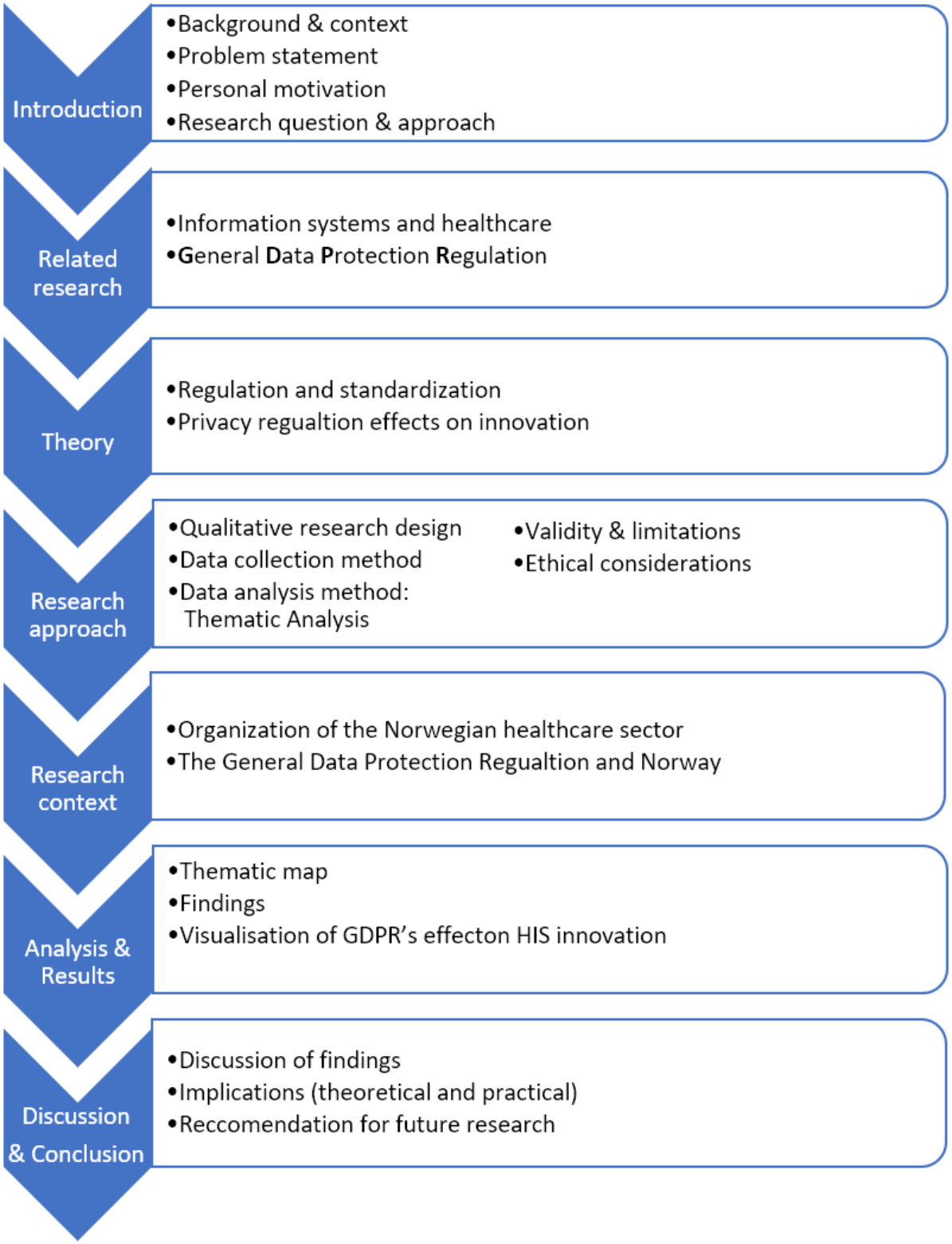


Figure 1.1. Flow diagram showing the overview of the thesis structure.

2. Background & related research

In this chapter, a literature review of related research on the topic is presented. In order to investigate how GDPR affects information system innovation for personal health information sharing initiatives, an understanding of the main basic concepts is thus needed; (1) Information systems and healthcare, (2) Health information system innovation, (3) General data protection regulation.

2.1 Information systems and healthcare

An information system through its definition can be explained as *"a set of interrelated components that collect (or retrieve), process, store, and distribute information to support decision making and control in an organisation."* (Laudon & Laudon, 2016, p. 48). The information system receives input in the form of raw data or information. Through the processing of the data/information, meaningful information is then retrieved as output from the system. This information is used by organisations and individuals to counter the challenges posed by the environment. For the effective use of an information system, a good understanding of the organisation, management, and technology shaping the information system is needed. Organisations use information systems in numerous ways, from large ERP systems to AI, management makes decisions, plan strategies, and act towards solving problems. Information technology sets the infrastructure and design of the information system through hardware, software, and networking (Laudon & Laudon, 2016, p. 48-54). When discussing IS in a business setting, the socio-technical system (STS) perspective is adopted. In the field of information systems, the STS perspective is often used to describe and understand the complex combination of technology, organisations, and people. STS sees an organisation as a combination of technical and social parts, and this combination is affected by the environment. The environment changes and an organisation may have a competitive advantage or disadvantage, changing levels of productivity or weaknesses. The environment will affect how management approaches problems, solutions, and make plans. Management decisions towards specific goals affect employees, and employees' attitudes towards the organisation are based on effects from the environment, decisions of the management, and technology used. Technology and the procedures and processes in an information system must adapt to reach the organisational goal, and the design of the systems and changes that may occur will affect people and management. It may also change the effects the environment has on the organisation (Appelbaum, 1997, p. 452-461). Information systems and the use of such technology is a complex topic. Still, the advantages of IS have resulted in IS being widely used and developed in numerous sectors and fields, among them the health sector. Electronic health (eHealth) is the use of information and communication technology (ICT) to provide better healthcare, with systems and technology that aids the processes within healthcare, providing storage, processing, information presentation, and communication to the actors involved (Swinkels, 2018). The term telemedicine is used by some to describe the health services delivered to patients from a distance. Telehealth is used as a broader term, including administration and education. The terms health information technology and health information systems are often used to describe healthcare combined with technology (Sligo, Gauld & Villa, 2017, p. 87). The use of technology within healthcare is viewed as a tool to help human activities, to assist in the computing of data, the quality and speed of work processes, and their outcomes. The term eHealth has had variable definitions throughout the years and is understood differently between individual actors. Still, it is commonly used as a broad term to describe the use of technology within healthcare (Oh, Rizo, Enkin & Jadad, 2005). For this study, we will be

using the term health information system (HIS) to collectively describe the use of information systems within healthcare.

2.1.1 Health information systems

HIS is the use of information systems within healthcare. Throughout this study, the following definition of HIS will inform the use of the term:

> "*HIS assist healthcare organisations to gather, process, and disseminate information within the organisation and their environment. HIS incorporates a range of different types of systems, which include patient information systems, administrative systems, radiology and pharmacy information systems, telemedicine and hospital information systems, such as computerized physician entry systems.*" (Sligo et al., 2017, p. 87)

The rationale of HIS is in simple terms to assist in more efficient and good quality healthcare for patients. HIS enables this through supporting tasks for medical and nursing personnel, as well as supporting the management and administrative tasks needed to provide efficient care for patients. The use of HIS developed over time, and from the 1960s and towards today, information systems (IS) in healthcare has rapidly evolved. Starting as minor applications and departmental information systems, it quickly evolved to include hospitals as a whole, namely hospital information systems. With a focus on developing patient-centred information systems and collaboration on regional, national, and international arenas, larger systems were researched and developed, resulting in the broader term health information systems (Haux, 2006, p. 271-272).

2.1.2 Privacy concerns in specific types of health information systems

There are some types of health information systems that have had a more prominent presence in research regarding privacy concerns. Following is a brief description of the type of HIS, and what aspects of GDPR concerns they are related to.

Electronic Health Records / Electronic medical records

A central component of utilising HIT to its full potential is the usage of Electronic Health Records (EHRs). An EHR is an information system that supports the delivery of personal healthcare services. This includes; delivery, care management, care support services and administrative processes. EHRs also have significant secondary uses as individuals more actively take part in the management of their own health. Moreover, education, regulation and health services research are secondary uses of EHRs. EHR address two types of users; (1) individual users (patients, clinicians, managers), and (2) institutional user (hospitals, public health departments, accreditation organisations, educators, and research entities) (Silverman, 2013, p. 2.).

Over the past decades, the definition of what EHR is used for has split up in two terminologies. This was a natural process to differentiate between the digitized systems used by care providers primarily for diagnostics and treatment, now known as Electronic Medical Records (EMR), and the aforementioned broader term Electronic Health Records (EHR) which include EMR information but also reach out beyond the health institution that collected the data. By virtue of mobile applications and the Internet of Things (IoT), EHR can support preventive care, nursing home care, and collaboration between clinicians across different health organisations (Silverman, 2013, p. 2-3.). Concerns were raised on how privacy issues may impede the diffusion of EHRs, but EHRs became widespread and seen as

a standard platform in the industry (Angst & Agarwal, 2009, p. 340-341). EHRs/EMRs have significant benefits that catalysed healthcare services for the general population. However, the sharing of personal health data among actors such as service providers, health professionals, health information networks and patients, is accompanied by the challenge of the sensitivity of personal data, which raises concern from personal data protection laws. Specifically, the GDPR explicitly provides reference to the principles of basic health data protection. Four standards are central in this matter; purpose limitation, data minimisation, proportionality and control (Yuan & Li, 2019, p. 4-5).

CDSS

Clinical Decision Support Systems (CDSS) are information systems designed to impact clinicians' decision making about specific patients in the moment that decisions are made (Berner, 2007, p. 3). CDSS differentiate from other clinical systems since they do not rely on retrospective analyses of financial and administrative data. Instead, they tend to utilise sophisticated data mining techniques (Berner, 2007, p. 3). CDSSs are unique in their timing since they may actively provide alerts or passively respond to the healthcare personnel input or patient information. There are two main branches:

(1) Knowledge-Based Clinical decision Support Systems. When developing this type of CDS, the aim was to assist the clinicians in their own decision making. Rather than coming up with the «answer», the system was expected to provide information for the user. With this as a limitation, the user was then expected to discard useless and erroneous information (Berner, 2007, p. 4). The knowledge-based system is dependent on compiled information and rulesets such as an IF-THEN rule. (Berner, 2007, p. 4-5).

(2) Nonknowledge-Based Clinical Decision Support Systems. This particular branch utilises technologies such as AI or machine learning (ML), which allows the system to learn from previous experiences. Additionally, the system can be used to recognise patterns in clinical data. Artificial Neural Networks (ANN) are the basis of a specific type of nonknowledge systems. Instead of giving decision support derived from medical literature or expert knowledge, the ANN analyses patterns in patient data to infer associations between the patients' signs, symptoms and diagnosis. An ANN consists of three layers; input, hidden layer, and output. Regarding privacy, the hidden layer is what has raised concerns. (Berner, 2007, p. 6). This hidden layer is also commonly referred to as "black box". The term "black box" is used because it is not possible to identify what attributes or nodes of data, or a combination of data, is used to create the result (Datatilsynet, 2018). How AI or similar technologies process and produce results pose large problems with complying to GDPR's principle of transparency and accountability (EU) 2016/679, 2016, p. 7, 11).

RPM

Unlike telemedicine, which is a reactive approach to healthcare, Remote Patient Monitoring (RPM) is generally proactive. Utilising networking technology and IoT devices such as sensors, health personnel can periodically monitor and measure the patients' health status. With this proactive method, necessary measures can be taken beforehand, prior to the full manifestation of a disease. This type of health service has helped relieve some of the pressure on hospitals, as patients with latent or mild conditions do not have to be hospitalised. Clinically, it can help prevent further spreading of diseases, as well as giving patients the security and comfort of their home (Pramik, Pareek & Nayyar, 2019, p 203-207). For RPM, there have been apparent challenges with complying to the GDPR related to both, explicit consent from the users for accessing and processing their data, and also, related to the possibility for a transparent method of revoking said consent (Pramik et al., 2019, p 222).

2.1.3 Health information systems innovation

Throughout history, there have been many different definitions of the term *innovation*. While there have been thoughts about the process itself, even before the term *innovation* was coined, we focus on the prominent definitions from literature in the last century. Zahra and Govin (1994, p 183) suggested that "*innovation is widely considered as the lifeblood of corporate survival and growth."* Furthermore, innovation is recognized to play a central role in value creation and gaining competitive advantage (Baregheh, Rowley & Sambrook, 2009, p.1324). On what role innovation has on renewal and growth, Phillips, Lamming, Noke & Bessant (2005, p. 1366) state that "*Innovation represents the core renewal process in any organisation. Unless it changes what it offers the world and the way in which it creates and delivers those offerings, it risks its survival and growth prospects".*

Before an innovation can become a sustainable product or service, it must go through several development phases. Most innovation that gains market traction and becomes a success has gone through a formal structural process (Menon Economics, 2019, p.46).

Patience and venture capital are key components in taking the project or organisation from research to commercialization. Venture capital can be difficult to acquire depending on how long the innovation process is and the uncertainty regarding the innovations market value. As a result of this, the innovation clusters and public innovation-organisations are important as many scientists and innovation-founders need help in the shape of guidance, network, and capital (Menon Economics, 2019, p.46).

In the last two decades, HIS has produced several new technologies. The background for this rapid development is based on innovations in telecommunications and information technologies (Daim, Behkami, Basoglu & Kök, 2016, p. 190). As the healthcare process is becoming more complicated, healthcare providers and patients need more collaboration and communication than ever before. EHR is an important factor and layer to establish and bridge these needs (Daim, Behkami, Basoglu & Kök, 2016, p. 190). In recent years innovations connected to handling big sets of data that are difficult to manage, store and process through traditional data processing techniques and platforms (Big Data) have emerged (Manogaran & Lopez, 2017, p. 183).

2.1.4 Challenges for health information system implementation

HIS solutions are developed and used to aid medical personnel, patients, administration, and management in providing quality healthcare. However, when planning, developing and implementing HIS, several challenges may arise that may inhibit or cause the projects to stop or be abandoned altogether. Many challenges related to the context and sociotechnical aspects of HIS, but some challenges may also be purely technical (Sligo et al., 2017, p. 92).

A literature review (Christensen & Næss, 2019) for the pilot project of this thesis revealed several challenges for HIS implementation. Thirty-five barriers to HIS implementation were identified and categorized in six overarching themes: (1) Planning, (2) Financial, (3) Architecture, (4) Management, (5) Implementation, and (6) Policy and Security. The findings revealed the challenges and barriers that might contribute to the failure of HIS implementation (Christensen & Næss, 2019). This literature review helped us gain an understanding of the overall challenges innovators, management, development teams, and organisations might face in the innovation process and orientate our attention towards investigating specifically how GDPR affects HIS innovation. Specifically, we identified a gap in the literature related to the role of GDPR and its effect on HIS innovation.

Interestingly, we did not find any prior related research. Also, it should be noted that more general research connected to policies and security was found to be an under-represented category in the literature review.
See an overview of the challenges in Table 2.1.

Literature search and revisions

The literature search and revisions for the literature review were based on Webster & Watson (2002, p. 15-21) and followed a structured approach. The overall process was conducted in multiple steps:

1. Identifying peer-reviewed journals within the field of information systems and HIS.
2. Search in the journal databases Scopus and AISeL with search strings based on criteria relevant to the studied field and scope.
3. Refine literature selection in 4 iterations (see Figure 2.1) based on title, journal, content, relevance. See Appendix B for an overview of selected literature.
4. Develop a concept matrix summarising the analysis of the reviewed literature, identifying concepts, theories and relevant meta-data. A template example of the concept matrix is shown in Figure 2.2.

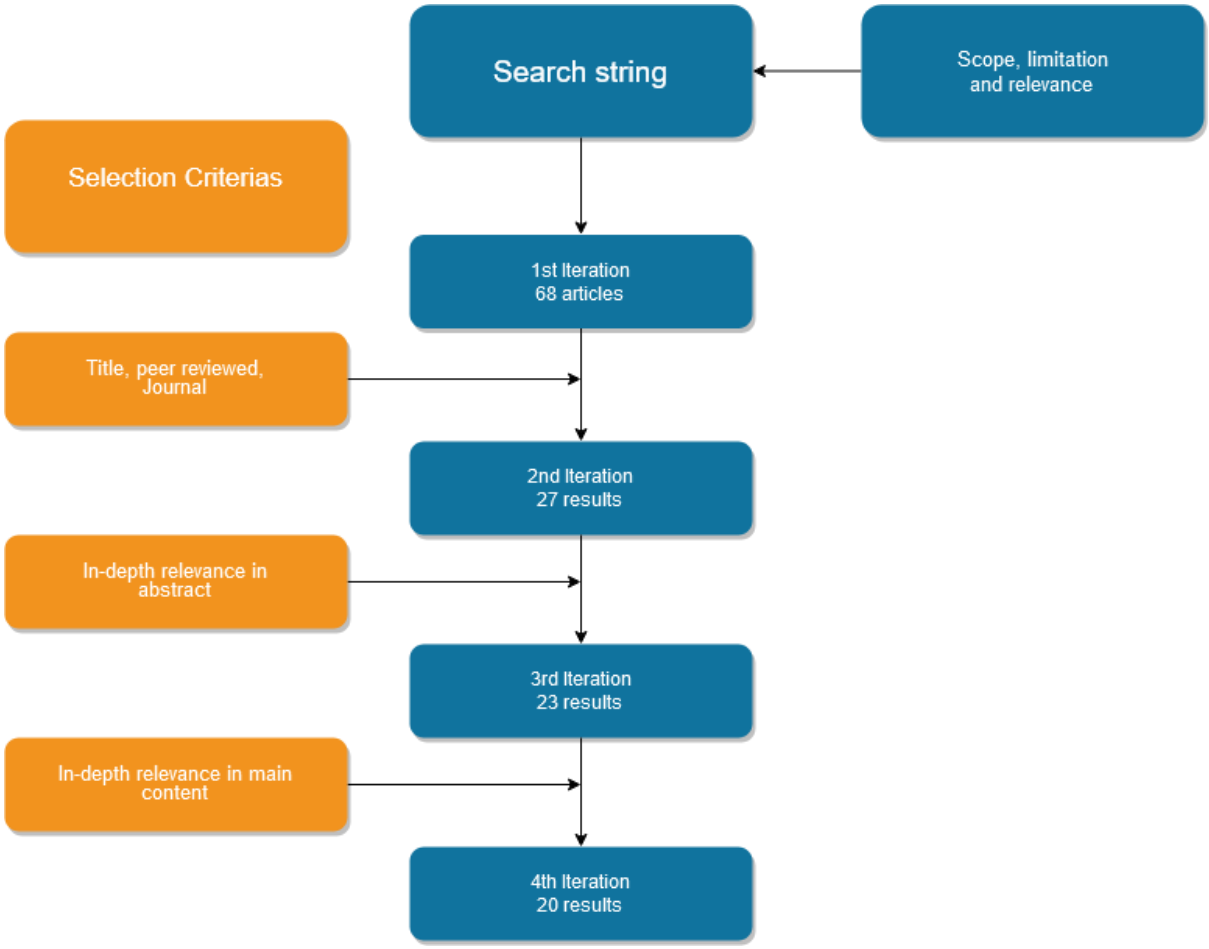


Figure 2.1. Iterative selection procedure from "Barriers in eHealth initiatives, a literature review", by F. Christensen and P. S. Næss, 2019, Unpublished manuscript, p. 5.

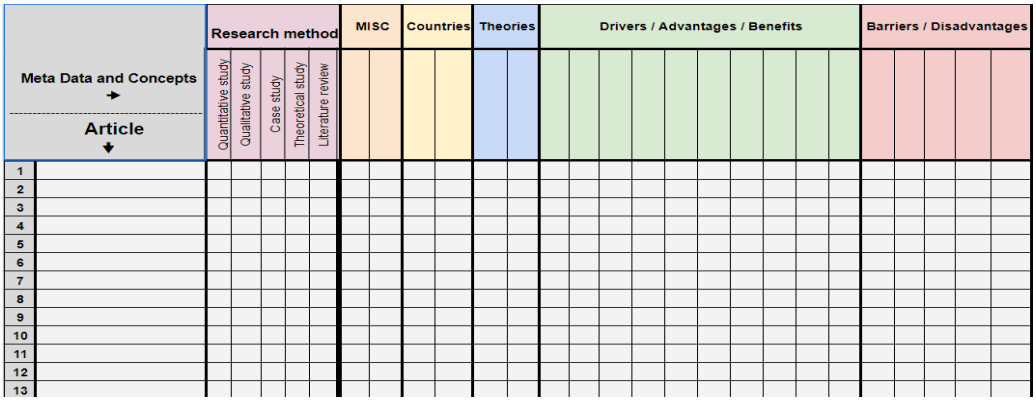


Figure 2.2. Literature concept matrix template from "Barriers in eHealth initiatives, a literature review", by F. Christensen and P. S. Næss, 2019, Unpublished manuscript, p. 3.

Results of the literature review

The themes and barriers for HIS identified through the literature review are presented and discussed in the following paragraphs.

Implementation

One of the most substantial identified barriers to HIS implementation is not including end-users. End-user involvement throughout the development and implementation of a HIS innovation project raises the quality of the product and the desirability to use the end-product (Sligo et al., 2017; Knight, Szucs, Dhillon, Lembke & Mitchell, 2014). Throughout the project's life-cycle, the collaboration between stakeholders is vital to make an end-product that is accepted by all parties (Swinkels et al., 2018; Vassilakopoulou, Grisot & Aanestad, 2015). Further, unexpected difficulties during the implementation, unexpectedly high costs and inadequate support during implementation can negatively affect the implementation process and act as barriers towards implementation (Shen et al., 2012, p. 220). Depending on inter-organisational innovation, not meeting project requirements, heterogenous development cycles, time misalignment (Hardless & Jaffar, 2011), low reliability and not focusing on and having inadequate education and training during the implementation process (Ariens et al., 2017) all act as barriers for HIS innovation.

Management

Poor leadership is a dominant barrier to HIS implementation. Effective communication with strong top-down leadership guidance is required for successful HIS implementation (Sligo et al., 2017; Speck, Weisberg & Fleisher, 2015). Poor or lack of change management and stakeholder management is a barrier, as stakeholders might have different expectations for the HIS, and staff reluctant to change as stakeholders may impose a culture which is different from the culture of the staff (Bidmead, Reid, Marshall & Southern, 2015,p. 156).
It can be challenging to commit to new solutions or change vendor while under contractual obligation, and it may be unclear who will manage the HIS implementation. Thus, uncertainty in ownership or long-term contracts pose a threat against HIS innovation. (Hardless & Jaffar, 2011).

Planning

The aspect of timelines, and specifically unrealistic timelines, can result in project failure or project abandonment. As a project is prolonged over the scheduled time, the project will rapidly see transgression of cost and time appropriated to the development and implementation of the HIS (Sligo et al., 2017). Furthermore, this leads to development time

misalignment, where the development and implementation teams are dependent on modifications by the receiving actor while the receiving actor is not ready to deliver these modifications, hence resulting in delayed delivery of the project (Hardless & Jaffar, 2011). According to Misser, Jasper, Van Zanne, Grooszen & Versendaal (2018), implementation processes are in many cases, rushed and lack sufficient planning, resulting in challenges that may ultimately cause the project to fail.

Policy and security

End users might not adopt or use HIS. This can, in part, be a result of unclear privacy measures in the system and a conception of low-security prioritization in HIS innovation initiatives. An effect of this is that a HIS innovation initiative might fail if the end-product is not used. Clear policy guidance in HIS initiatives is important to succeed with HIS innovation (Kenny et al., 2017). End-users, healthcare professionals and SMEs must collaborate with policymakers to design acceptable policies (Swinkels et al., 2018). A further barrier is the lack of data ownership and governance, making it unclear who owns the data. This can result in stakeholders not adopting the innovation initiative (Ariens et al., 2017).

Financial

Countries use only limited amounts of their total health budgets towards digitalization in the health sector, and the implementation of HIS can be expensive. Often, costs that may appear during the implementation of HIS initiatives are not accounted for in the planning phase of the innovation project, resulting in costs exceeding the expected and budgeted amount when implementing the system (Sligo et al., 2017). Minimising sunk costs that make affordable losses, in turn, make the initiatives vulnerable, by going for the cheapest alternatives or creative ways of doing things at no cost for a specific stakeholder. Large-scale investment is vital for anchoring the project and securing the project from being scrapped before it delivers benefits (Vassilakopoulou, Grisot & Aanestad, 2015). Stakeholder concerns are high-costs and cost-effectiveness in HIS initiatives, and this can put pressure on, or limit the use of, resources in a HIS innovation process (Ariens et al., 2017).

Architecture

A bottom-up approach has been shown to be suitable for developing IT/IS infrastructure. The infrastructure must be loosely coupled, and it is vital that the infrastructure is flexible and straightforward. Easy to use solutions are required for innovation projects to integrate new systems and models to already existing infrastructure (Grisot, Hanseth & Thorseng, 2014). New pilot projects may be blocked by existing infrastructure and not fully implemented when there is lacking a sound groundwork for the infrastructure (Speck, Weisberg & Fleisher, 2015). A scalable architecture that can handle a growing number of users is vital to be able to maintain and improve the solutions (Grisot et al., 2014). Further, both physical and virtual grounds for communication and collaboration must be available, as not having a physical location for actors to meet in multidisciplinary cooperation may hinder the projects. The inclusion of end-users in the collaboration is also essential to provide possibilities for improved quality of the innovation (Speck et al., 2015).

Literature gap and potential basis for further research

With the aforementioned barriers in mind, a gap in the literature has been identified. Through the literature review, no articles discuss how the GDPR affects innovations in the health industry. When reviewing the literature, eight of the articles reviewed were published after GDPR was introduced in the EU (European Data Protection Supervisor, 2019). However,

none of them address the regulation as a potential barrier for innovation. Furthermore, research on barriers connected to policies and security was found to be an underrepresented category in the literature review. There is a need for investigation on the effects of GDPR.

Table 2.1. Categories (headings) and barriers (subheadings) from "Barriers in eHealth initiatives, a literature review", by F. Christensen and P. S. Næss, 2019, Unpublished manuscript, p. 15.

Challenges for HIS implementation overview - Barriers in each category	
Financial	**Architecture**
High costs	Infrastructure
Vulnerable initiatives due to affordable losses	Unchangeable/unscalable ICT architecture
Cost-effectiveness	Lack of physical environment for cooperation
Management	**Implementation**
Poor leadership	Inadequate end-user engagement
Staff reluctant to change	Difficulties in implementation
Competing demands	Inadequate support services
Governance processes	Not meeting requirements
Lack of culture regarding information sharing	Dependency on inter-organisational innovation
Uncertain ownership of implementation	Infrequent use
Long term contracts	Heterogeneous development cycles
Cultural barriers	Low end-user acceptance
Policy and security	Lack of education and training
Lack of policy guidance	Reliability of HIS
Poor security and privacy	Problems with technology
Uncertain/lack of data ownership/governance	Data quality during and after implementation
Confidentiality	
Planning	
Unrealistic timelines	
Cautious exploration targeting market needs	
Lack of research/methodologies	
Procurement boundary spanning	
Decentralized procurement	

2.2 General data protection regulation

The European Community (now *EU*) had, for several years, felt the need to align data protection standards across their member states in order to realise cross-border data transfers. In the early 1990s, no specific international data protection laws regulating personal data in the EU were present. Different countries had different national data protection laws, where some provided considerably different levels of protection and could not offer legal certainty (Voigt & Von dem Bussche, 2017. p. 1-2). The European Community answered this challenge by adopting *Directive 95/46/EC* of the European Parliament and Council on the 24th of October 1995. This new directive would be called the *Data Protection Directive*, and its purpose was to protect individuals with regards to the processing of personal data and of the free movement of such data. Furthermore, the directive sought to harmonise the protection of fundamental rights of individuals regarding data processing activities and ensure a free flow of personal data between EU member states (Voigt & Von dem Bussche, 2017. p. 2). The Data Protection Directive did not meet the goal it set out to achieve. It failed in the aim of aligning the level of data protection within the EU. Several legal differences arose as a consequence of the trans-national implementation. Due to different legislation and laws amongst the member states, specific execution of data processing could be legal in one state, but unlawful in another. This failure set the stage for a completely new regulation (Voigt & Von dem Bussche, 2017. p. 2).

The General Data Protection Regulation (GDPR) is the latest juridical action in the ongoing global recognition of the value and importance of personal information. While the information economy has existed for some time, the real value of personal data has only recently become evident. With the significant increase of cyber-attacks on ICT infrastructure in recent years (Politidirektoratet, 2017, p.8), EU citizens are being exposed to significant personal risk (IT Governance Privacy Team, 2017, p. 11). Voigt & Von dem Bussche (2017), explain how data over the last couple of years has been called “the currency of the future.” The reasoning for this is that data, in its very nature, can easily cross borders and play a vital role in the global digital economy.

2.2.1 Principles of the GDPR

The GDPR is based on six general data protection principles for personal data, with data protection by design and default as the basis for the regulation. The six principles are: (1) fairness and lawfulness, (2) purpose limitation, (3) data minimisation, (4) accuracy, (5) storage limitation, and (6) integrity and confidentiality; as described in Table 2.2 from article 5 of the GDPR (Regulation (EU) 2016/679, 2016, p. 35-36).

Table 2.2. The six principles of GDPR

Fairness and lawfulness	"*Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');"* (Regulation (EU) 2016/679, 2016, p. 35)
Purpose limitation	*"collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');"* (Regulation (EU) 2016/679, 2016, p. 35)
Data minimisation	*"adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');"* (Regulation (EU) 2016/679, 2016, p. 35)
Accuracy	*"accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');"* (Regulation (EU) 2016/679, 2016, p. 35)
Storage limitation	*"Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to the implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');"* (Regulation (EU) 2016/679, 2016, p. 36)
Integrity and confidentiality	*"processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."* (Regulation (EU) 2016/679, 2016, p. 36)

In addition, article 5 states that the controller, (that is agencies, public authorities, natural or legal persons or other bodies that alone or with others determines the means and purposes of the processing of personal data), is responsible and must show compliance with the principles, referred to as accountability. A processor is the same type of body as a controller, and a processor processes personal data on behalf of a controller. (Regulation (EU) 2016/679, 2016, p. 33-36). Data protection by design and data protection by default are principles introduced with the GDPR, and the purpose of these principles is to integrate privacy into the life cycle of technology that processes personal data (Jasmontaite, Kamara, Zanfir-Fortuna & Leucci, 2018, p. 1-2).

2.2.2 Practical implications of the GDPR

Data protection by design and data protection by default are, in practice, complex to abide by, because they are abstract and prone to uncertainty when it comes to the meaning of the principles, and they are often interpreted differently between actors (Jasmontaite et al., 2018, p. 1-2). The GDPR has had practical impacts on the design of technology and software. Tamburri (2020) identified several industrial design challenges that can be encountered and must be considered, in order to be compliant with the regulation. These include the following design issues: overcollection, distortion, appropriation, insecurity, unwanted disclosure, forced disclosure, unanticipated revelation and unwarranted restriction (Tamburri, 2020, p. 12). Tamburri (2020) claim that systems and software should be re-designed to make the role of data protection officers clear so they can do their duty, re-designed without prejudice to processing information about children especially, and re-designed to make use of security-enhancing approaches and middleware, and privacy-enhancing technologies to the benefit of the interested data subjects (Tamburri, 2020, p. 12).

Further, the GDPR affects technologies that leverage artificial intelligence (AI). The principles of fairness, purpose limitation and data minimisation impact the use of AI on personal data. The ML algorithms must not collect unnecessary data, not be skewed by putting analytic emphasis on race, religion, political opinion, health condition or sexual orientation by the principle of fairness. The data used must be necessary and relevant and not go beyond the original purpose. Therefore, the continuous evaluation of the necessity to use the data must be done, in accordance with the principle of data minimization and purpose limitation. In addition, GDPR triggers an extended information duty for the developers and users of AI to inform data subjects of their rights, the purpose of using the data, right to data portability and categories of data being used when it comes to automated processes. This can be difficult with large amounts of data being processed by the AI. In addition, the complexity of ML algorithms can be hard to explain, and insight into the algorithms can expose corporate secrets and immaterial rights. The GDPR principles of transparent processing of data to inform data subjects applies fully to complex AI, and the black box issue of closed algorithms and the exposure risk of revealing algorithms is an issue. Developers of AI solutions must therefore find pragmatic solutions to inform data subjects without exposing corporate secrets (Datatilsynet, 2018, p. 14-18).

Several types of information systems are in one way or another affected by GDPR. Vast amounts of health data and the analysis of big data in health has shown great potential. However, there has not been a unified criterion for governing health-data. This leads to difficulties in data-sharing and patients' privacy protection. Identifying data can be revealed by intercepting multiple databases or complex statistical analyses, and thus privacy is a concern. There is a need for collaboration on big data and especially cloud solutions for big data among researchers and the public and private sector in the healthcare domain, as healthcare big data can bring several benefits for research within the field. There have been solutions to privacy concerns such as differential privacy, but these solutions are often too restrictive to be practically implemented (Gu, Li, Li & Liang, 2017, p. 30-31).

2.2.3 The GDPR and innovation

Although there is limited research in how the GDPR affects innovation for HIS, some research has been conducted related to innovation in general. Particularly relevant is the study by Martin et al., (2019) that explored how the GDPR affects start-up innovation and identified that the GDPR had both obstructing and stimulating effects on innovation. On the

stimulating side, they identified two key categories: a) compliance innovation, where one makes products compliant with the regulation, and b) regulation-exploiting innovation, where one innovates products that assist in achieving compliance for companies are driving innovation. An example of compliance innovation is the development of anonymization technologies, so one can provide analytics to customers that are regulation compliant. Regulation exploiting innovation has taken advantage of regulation to support data protection and compliance. A lot of third-party technologies have appeared, for data protection compliance management software, and IT/IS security products. The study found that an effect of GDPR was that companies started buying more products from the EU, as they were wary of using non-European providers that might be non-compliant and, for instance, using cloud-providers outside EU. The "Buy European" effect has hence driven a more Europe-centred market for innovation (Martin et al., 2019, p. 1317-1321).

The Martin et al. (2019) study found innovation constraining effects. Entrepreneurial discouragement, product abandonment, lack of a direct relationship to end-users or data-subjects, inability to offer users or data subjects direct and tangible benefits from the processing and data minimization were constraining effects on innovation. Some entrepreneurs might not endeavour in innovation initiatives due to the regulation. Products might be abandoned at the idea phase, due to customers not accepting because of non-compliance or uncertainty, and the costs of making compliant innovation can result in abandoned innovation projects. Innovations dealing with large amounts of data can be troublesome in the context of consent to use personal information, as with big data or AI that need a vast amount of data. Great amounts of data need to be collected from third parties, and so the regulation may negatively affect the sharing of datasets for analytical purposes. Data minimization may also negatively affect innovation, as there is a danger that companies might become "data-starved" and impact fields like AI, particularly. Users may also feel reluctant to share information and give consent if the data collection is excessive, and less data might make it harder to optimise products. Also, the need for a legal basis and the purpose-limitation principle can negatively affect innovation with regards to data-sharing (Martin et al., 2019, p. 1317-1321). Further, Martin et al. (2019) suggest future research to continue to study the effects of GDPR on innovation over a more extended period, in order to assess both long- and short-term effects. Furthermore, it is suggested to continue the research within other fields and contexts, to get a broader understanding of GDPRs impact on innovation.

3. Theory

This chapter presents the theoretical concepts guiding this thesis. We first present concepts introduced in prior research related to the impact of regulation and formal standardisation on innovation. These concepts are relevant, as the balance between regulation and formal standardisation impacts the efficiency of innovation. Furthermore, we present prior research conceptualisation of the role of privacy regulation, with the corresponding effect on innovation. These theoretical concepts, models and frameworks have been chosen to form the scope of research for this study, since the purpose of this thesis is to investigate how GDPR affects HIS innovation and what concrete responses companies apply to HIS initiatives to meet constraints set by the GDPR. Using these concepts as a basis for the analysis of this study's empirical data, will aid understanding of how the health sector regulates and enforces regulation concerning HIS innovation. These concepts can further be used to reveal the effects the GDPR has on HIS innovation, and if standards are used, or maybe should be used, for innovation of regulation-compliant HIS.

3.1 Regulation and standardisation

Regulation and standardisation can impact innovation. Drawing on the theoretical concepts of regulatory capture, where organisations try to influence regulation in terms of their own interest, and information asymmetry, where actors have a different level of knowledge in a technological frontier, Blind et al. (2017) present a model of direct governmental regulation and the impact of standardisation on innovation. The model suggests that regulation and formal standardisation have different effects on innovation efficiency in firms over different market environments. When studying a regulation's effect on innovation, it is essential to differentiate between regulation and standardisation (Blind et al., 2017, p. 249-252).

3.1.1 Regulation and innovation

Regulation is used to influence the actions and behaviour of actors in a market, and to shape the market environment. Regulation has a top-down approach, where governments issue regulations on the market, called a direct governmental regulation. A regulation is a mandatory legal restriction enacted and released by government authorities. Regulation has different impacts on innovation efficiency based on the market. Innovation success is dependent on the introduction of new products and the behaviour of the consumers. If there is low demand, it is harder to introduce new products to the market. Market uncertainty thus plays a significant role in regulations impact on innovation. Uncertainty can come from technological complexity, competition and user behaviour. A market with high uncertainty has unpredictable behaviour among consumers and technological heterogeneity, where different technological solutions compete, increasing the uncertainty for consumers and producers. There may be many technological products to choose between, resulting in consumers waiting on a dominant technological infrastructure resulting in consumers not investing in innovative products. Furthermore, unpredictable consumers make it difficult for innovators and producers to choose the technological path to invest in (Blind et al., 2017, p. 250-251).

The model by Blind et al. (2017) suggests that in markets with low uncertainty, regulation has a positive effect on innovation efficiency. The regulations have a closer connection towards the underlying technologies, with low information asymmetry. There is a minor misfit between regulation and the underlying technologies. Thus, regulation in a mature market creates non-discriminating and transparent rules. On the opposite side, in markets

with high uncertainty, regulation has a negative effect on innovation efficiency. There is a greater misfit between regulation and technology, and the regulation is not sufficiently matching the different emerging technologies. Because of the top-down approach of regulations, regulation will act more as a barrier for innovation in uncertain markets (Blind et al., 2017, p. 250-251).

3.1.2 Standardisation and innovation

According to Blind et al. (2017), standardisation has an impact on innovation efficiency. For standards, they describe what they call formal standards, which are consensus-driven standards, voluntary, made in standardisation bodies and can be seen as self-regulatory processes. Often, only a small amount of businesses are actively involved in developing formal standards. Regulations differ from formal standards, as the formal standards are usually the result of a market-driven process, such as industry self-regulation, while regulations are developed, enacted and enforced by governments from a top-down approach. Regulations are mandatory to follow, while formal standards are usually voluntary to follow (Blind et al., 2017, p. 250).

In a health context, standardisation has the intent to enable and support solutions that best contribute to the overall improvement of the healthcare sector through development or co-creation of new and improved medical services. In the Norwegian healthcare sector, the general picture of the field is that the general implementation and diffusion of standardisation have been very slow (Hanseth, Bygstad, Ellingsen, Johannessen & Larsen, 2012, p. 15). In most cases, ICT solutions are shared by most of the members in the business sector (i.e. healthcare). A by-product of this is a very complex development process because solutions tend to include a large number of technological components at the same time owing to a large amount of development and user organisations being involved (Hanseth et al., 2012, p.3). One of the main drawbacks of standardised systems is that, over time, they accumulatively become change-resistant as they grow and diffuse. According to Tassey (1995), this can be solved by having standards that allow for growth and change through different means of flexibility. Standardised interfaces, decomposition, and modularization allow for core components to be kept stable, while other components are available for change without compromising the system. The main benefactors of allowing for peripheral change and innovation can result in a significant increase in the size of the system, its market, as well as the diversity of services (Lessig, 2001).

In the model presented by Blind et al. (2017), it is postulated that standards increase organisations´ innovation costs more than regulation in markets with low uncertainty. More specifically, they stated that in markets with low or medium uncertainty, standards and regulation have comparable effects. In the case of markets with high uncertainty, Blind et al. (2017) identified the opposite effect. Regulation has a more significant impact on innovation costs and efficiency compared to standards.

3.2 Effects of privacy regulation on innovation

Regulation affects innovation based on market uncertainty, and this may also apply to GDPR. In their study, Martin et al. (2019) present a conceptual theoretical framework, where the regulatory enforcement of data protection law, combined with market demand for data protection law-compliant products, affect innovation. In environments with strict regulatory enforcement and high demand for compliant products, there is an incentive to innovate

regulation-compliant and regulation exploiting innovation, and little to no strategic gain to innovate non-compliant products. There is also a high level of innovation abandonment, thus negatively impacting innovation progress, but innovations that become implemented are highly compliant with the regulation. Regulation is thus both negatively affecting innovation and endorsing innovation of compliant products. With strict regulatory enforcement and low demand for compliant products, there is little strategic non-compliant, compliant and exploiting innovation. Furthermore, there is high innovation abandonment, and the regulation, therefore, reduces overall levels of innovation. Lax enforcement and high demand for compliant products lead to the highest level of overall innovation, and there can be both compliant and regulation exploiting innovation, as well as possibilities to innovate strategic non-compliant innovations. Here there are low levels of innovation abandonment. With lax enforcement and little demand for compliant innovation, one can expect high levels of strategic non-compliant innovations and low level of abandonment, and little incentive to innovate compliant and regulation-exploiting innovation. With lax enforcement and little demand, regulation thus has little effect, either negative or positive on innovation. Overall, GDPRs effect can be both constraining and stimulating for innovation. It depends on the demand for compliant innovation solutions and enforcement levels of the regulation (Martin et al., 2019, p. 1311-1312).

3.3 Summary

According to Blind et al. (2017), regulation has a negative impact on innovation in markets with high uncertainty and in such settings, there can be gains from market-driven standards. In mature, stable markets, regulations are more matched with the technology and have a positive effect on innovation (Blind et al., 2017). Privacy regulation can have both negative and positive effects on innovation. Depending on the level of regulation enforcement and demand for innovative, compliant products, privacy regulation can result in both high and low level of abandoned innovation projects, high and low strategic non-compliant, compliant and regulation exploiting innovations (Martin et al., 2019).

The remainder of this thesis focusses on the effect of GDPR on HIS innovation by considering empirical data gathered. In the following section, we present the method applied for the collection of data, before continuing with the context of the study in Chapter 5 and with a presentation of the results and discussions in Chapters 6 and 7.

4. Research approach

The research approach allowed us to investigate the effect GDPR has on HIS innovation in the healthcare sector. Specifically, we explored HISs processing large quantities of personal health data, while focusing on how the GDPR is dealt with in practice when implementing HIS innovation. The study poses two research questions in order to develop an understanding of the phenomena:

(1) How does the General Data Protection Regulation affect health information system innovation for personal health information sharing initiatives?

(2) What concrete responses do companies apply to health information system initiatives to meet constraints set by the General Data Protection Regulation?

In this chapter, the thesis's research approach is described, presenting the design and method of the research. The rationale of the research approach is discussed as well as the choice of interview approach, data collection process, analysis method, the validity of findings and limitations to the research approach. The chapter concludes with a discussion on ethical considerations raised by the research approach.

4.1 Qualitative research design

This master thesis is based on qualitative research methods. Qualitative research is intended to explore the world, not from artificial settings, e.g. laboratories, but to understand, describe and explore the social phenomena from the inside. In qualitative research, the researcher is interested in accessing documents, interactions and experiences from the natural context which they come from. One seeks to unpick how people construct the world around them, what is happening to them, and what they are doing, in ways that are meaningful and offer rich insight (Flick, 2007). Although there are many philosophical paradigms within qualitative research, Oates (2006) presents three main paradigms used within information systems research: positivist, interpretive and critical.

Positivism is based on two underlying assumptions that (1) the world is not random; it is ordered and regular, and (2) the world can be investigated objectively. The aim is to find universal laws, regularities and patterns that are generalisable. The world exists independently of humans. Interpretivism does not prove or disprove hypotheses, as in positivism, but acknowledges that there is no single version of the truth. What is real and knowledge is a construction of the mind; groups and culture experience the world differently. Critical research seeks to identify power relations, contradictions and conflicts, and give power to the people as to eliminate them from being sources of domination and alienation. Social reality is created by people, but social reality also has objective properties, dominating the way the world is seen and experienced, such as cultural, economic and political authority. Critical research does not accept the status quo, but questions and challenges it (Oates, 2006, p. 283-297).

In this study, the informants are assumed to have subjective interpretations of the world around them. Their beliefs and experiences will be individual and made up of the social constructs around them, and reality can only be transmitted on through further social constructs. We report and analyse based on our interpretation of the data we collect, bringing our own interpretation into the research. To be able to do this, we must develop an understanding of the context within healthcare, innovation, information systems, and the GDPR. We seek the experiences of people within HIS innovation initiatives, and their

experiences of the GDPR and how GDPR has affected them and their projects, as well as their interpretation of GDPR. We seek the participants' point of view within this context and their interpretation of the reality in this context. This study does not embrace the positivist paradigm seeking to find the objective reality, nor does the study aim to reveal power relations, empowering people who are alienated and dominated, critiquing the status quo. The study seeks the experiences and views of the informants, their reality combined with the interpretation of us conducting this research, accepting that there is no single truth, and there may be multiple interpretations. Therefore, this study assumes the interpretive paradigm, and a qualitative research method is deemed appropriate (Oates, 2006, p. 292-296).

4.2 Data collection method

Since we are utilising a qualitative approach and can be positioned in the interpretive paradigm, the strategy for data collection implemented in this research design is qualitative data collection through semi-structured interviews. This strategy is in line with what our research design wants to accomplish. In addition, it is in line with what Oates (2006, p. 187) describes as suitable if the researcher wants to:

(1) obtain detailed information,

(2) ask questions that are complex, or open-ended, or whose order and logic might need to be different for different people,

(3) explore experiences that cannot easily be observed or described via pre-defined questionnaire responses,

(4) investigate sensitive issues, or privileged information, that respondents might not want to disclose in writing to an interviewer they have not formerly met.

Connected to qualitative interviews, a set of assumptions, which are not present in normal conversation, is apparent. In most cases, the interviewer has a particular purpose for undertaking the interview; to gain relevant information from the interviewee. Since the interviewer has planned the interview, the discussion does not occur by chance. The interviewer has an agenda, specific themes and issues he wants to discuss, so the topics up for discussion does not occur arbitrarily or randomly. The researcher guides the discussion through predetermined topics. In contrary to a free-flowing conversation, there is a tacit agreement that at the beginning of the interview, the researcher will steer and control both the agenda and the proceedings, as well as ask most of the questions (Oates, 2006, p. 186).

4.2.1 Interviews

To answer the research questions stated in Chapter 4, we conducted 11 semi-structured interviews. A semi-structured interview, in contrary to structured interviews which use pre-determined, standardised, identical questions for every interviewee, have a list of themes or topics to be covered and questions that are related to them. The interviewer must adapt and change the questions depending on the flow of the interview. The semi-structured approach is also a good fit if the interviewee brings up issues or topics that had no prepared questions for (Oates, 2006, p.188-189). In the context of this master thesis, where we as interviewers are not experts in the domain, the semi-structured interviews allowed us to explore both the pre-determined topics we have identified through literature, but also allowed for the interviewee to raise own issues or topics that have not earlier been identified through literature. It is important to note that the interviews were conducted in Norwegian. Quotes in the result chapter will be translated to English to fit the thesis audience.

The subjects for interviews can be put into two categories: (1) Healthcare, and (2) Healthcare software/solution suppliers. These interviews will give insight to what underlying barriers related to regulation and GDPR limits potential novel HIS initiatives conducted in both public and private healthcare. By including both categories in our study, we can expose which constraints for both data-processors and data-controllers are. In addition, we can explore and compare how both categories understand and interpret the regulation. Furthermore, the interviews can give insights to the use of frameworks, analysis and guidelines.

4.2.2 Data collection process

The identification of candidates has been approached in a few different ways. (1) Internet research. For our initial search for candidates, we identified some of the local organisations that we knew had projects related to eHealth information systems. (2) Networking. We have utilised our own networks but also the networks of central persons from the institute for information systems. The University of Agder has a vast network in the national eHealth sector. (3) Snowballing. Through specific interviews, the interviewees recommended us candidates who can contribute to providing a good picture of the current state in the Norwegian eHealth sector.

Mainly, our interview candidates have been approached through e-mail. In some cases, due to the circumstances, we utilised phone calls to invite and make arrangements for the interview. We strived to have as many of the interviews in person and approximately 50% were conducted face-to-face. The remaining interviews were conducted through video conferences. The high percentage of interviews conducted through video conferences can, in some part, be contributed to the outbreak of Covid-19. To record the interview, we are imposed by the University of Agder and Norsk Senter For Forskningsdata (Norwegian Center For Research Data, NSD) to use a dictaphone. This dictaphone must be supplied by the university and cannot be an IoT device (no network connection). The reasoning for this is the confidentiality of our informants and the means to ensure no leakage of data collected. Recorded interviews are transferred to UiA's secure Office 365 platform. When the project date expires, raw data (audio files) will be deleted to ensure privacy. This is in line with the guidelines from NSD and our declaration of consent.

4.2.3 Data sources

The empirical data for this study were collected through 11 interviews with nine interviewees in eight companies from the public and private healthcare sector with a focus on HIS. Table 4.1 present the data sources for this study.

Table 4.1. Data sources

Company number	Interviewee number	Role	Int. count	B2B/B2C*	Industry	Sector
Company 1	Interviewee 1	Management	2	B2B, B2C	Public healthcare	Public
	Interviewee 2	Privacy and data security	1	B2B, B2C	Public healthcare	Public
Company 2	Interviewee 3	Privacy and data security	1	B2B, B2C	Municipality	Public
Company 3	Interviewee 4	Management	1	B2B	IT service provider and consultancy	Private
Company 4	Interviewee 5	Privacy and data security	2	B2B	IT service provider and consultancy	Private
Company 5	Interviewee 6	Management	1	B2B	Medical technology	Private
Company 6	Interviewee 7	Management	1	B2B	Medical technology	Private
Company 7	Interviewee 8	Management	1	B2B, B2C	Municipality	Public
Company 8	Interviewee 9	Privacy and data security	1	B2B, B2C	Public healthcare	Public

*** B2B = Business to business / B2C = Business to consumer**

4.3 Data analysis method: thematic analysis

The analysis of the collected data from this study was conducted using a thematic analysis method. We adopted the approach of Braun and Clarke (2006) to thematic analysis, as it is a fairly open method within qualitative research. It is a method for identifying, analysing, and reporting themes (patterns) within the data corpus (all collected data) and dataset (data from data corpus for a particular part of the analysis). The analysis method is useful both for the experienced and the newcomer within the world of qualitative research analysis. Thematic analysis is not tied to any pre-existing theoretical framework, and thus can be used within a number of theoretical frameworks. It can be an essentialist or realist method, a constructionist, or a contextualised method (Braun & Clarke, 2006, p. 4-9).

The essentialist or realist method, reports meanings, the reality of participants, and their experiences, whereas the constructionist method looks at the effects that realities, meanings, experiences, and events have on discourse within the society. The contextualised method is in between the other methods, as it looks at how people make meaning of their experiences, and how those meanings impact a broader social context while still having a focus on the limitations and material of reality, often characterized by theories like critical realism. The thematic analysis can thus both reflect reality and go beyond the surface of reality (Braun & Clark, 2006, p. 9).

This study used the model of standardisation and regulation by Blind et al. (2017) and conceptual framework of Martin et al. (2019), and the underlying theoretical assumptions for our research scope, and is hence a deductive, top-down approach to analysis. The research was based on our theoretical and analytical interest in the topic of this study, giving a more analyst-driven approach. As this study assumes an interpretive philosophical paradigm, where we, using theory and own interpretation, seek to identify the underlying ideologies, assumptions, ideas and concepts, to understand the particular form and meaning of the phenomena under study. The analysis of the data corpus and following datasets was therefore conducted on a latent level, rather than a semantic level that reports the surface of the data, where latent analysis explores beyond the surface. This, in turn, made the analysis approach lean more towards the constructionist method, rather than an essentialist or contextualised method (Braun & Clark, 2006, p. 9-17).

The thematic analysis sought to identify themes (patterns), and it was thus essential to describe what a theme is, and the size of a theme. In this context, a theme captures something important about the data. The theme is in relation to the theory and research questions and represents a meaning or a pattern within the data set. As to the size of a theme, there is no set standard, and the theme needs to be flexible, as strict restrictions to the size of a theme can bias the meaning it represents and goes against the interpretive, qualitative approach to the analysis. The weight of a theme is not quantifiable; the importance of a theme lies in how well it captures information of importance regarding the overall research question. An overarching theme may also contain underlying sub-themes, thereby enriching and giving a more in-depth analysis of the dataset being analysed (Braun & Clark, 2006, p. 10-11).

4.3.1 The analysis process

The analytical process of thematic analysis follows six phases as presented in Table 4.2: (1) Familiarize yourself with your data, (2) Generate initial codes, (3) Search for themes, (4) Review themes, (5) Define and name themes, and (6) Produce the report (Braun & Clark, 2006, p. 87-93).
(1) In phase one, the data is transcribed from the raw audio files containing the recordings of the interview. In this initial phase, transcripts are read and re-read, and one starts to envision what codes lies within the data, trying to understand the depth and meaning of the data while forming ideas and identifying patterns within the data (Braun & Clarke, 2006, p. 87-93).
(2) In phase two, one starts to code the data, identifying features of the data, representing the basic segments or elements of the raw data. The codes differ from themes as themes are broader than codes (Braun & Clarke, 2006, p. 87-93).
(3) In phase three, one starts searching for themes. The themes can be identified by analysing the list of codes identified in phase two, covering several codes that make up the broader theme. After this phase, one has a list of candidate themes, which contains underlying themes and all the codes from the raw data (Braun & Clarke, 2006, p. 87-93).
(4) In phase four, one review all the candidate themes. Some themes might not actually be themes, and other themes might be so close to each other that it is more meaningful to merge them into one theme. Other themes might be discarded all together. All material is re-read as to discover themes, and discover possible new codes that fall within newly created themes. At the end of this phase, a candidate map of themes has been created, which can be analysed at a top-level, to check the validity of the themes in regards to the datasets, that the themes represent the overall flow of the data corpus, and if the themes are an accurate representation of the theoretical and analytical approach. The themes should be differentiable, fit together,

and show the overall story of the data (Braun & Clarke, 2006, p. 87-93).
(5) In phase five, one analyses the thematic map, checking that the themes are not too diverse and complex, not trying to get the themes to do too much. In this phase, one identifies the overarching themes, and what themes may be sub-themes in the overarching themes. It is crucial to interpret and understand the story of a theme, by thoroughly analysing each theme, understanding the what and why of the narrative the theme tells, not just paraphrasing the content. One should be able to tell what the theme "is", and "is not", and final names for the themes can be set (Braun & Clarke, 2006, p. 87-93).
(6) In phase six, the final phase, one presents the results of the analysis, telling the complete and complicated story of the data convincingly, underscoring the validity and merit of the analysis. The report of findings must show a logical, coherent, non-repetitive, and consistently interesting story of the data, underscored by examples from the raw material that best represents the meaning and significance of the theme (Braun & Clarke, 2006, p. 87-93).

Table 4.2. Phases of Thematic Analysis. From "Using thematic analysis in psychology" by V. Braun and V. Clarke, 2006, Qualitative Research in Psychology, 3(2), p. 87.

Phase	Description of the process
1. Familiarising yourself with your data:	Transcribing data (if necessary), reading and re-reading the data, noting down initial ideas.
2. Generating initial codes:	Coding interesting features of the data in a systematic fashion across the entire data set, collating data relevant to each code.
3. Searching for themes:	Collating codes into potential themes, gathering all data relevant to each potential theme.
4. Reviewing themes:	Checking in the themes work in relation to the coded extracts (Level 1) and the entire data set (Level 2), generating a thematic 'map' of the analysis.
5. Defining and naming themes:	Ongoing analysis to refine the specifics of each theme, and the overall story the analysis tells; generating clear definitions and names for each theme.
6. Producing the report:	The final opportunity for analysis. Selection of vivid, compelling extract examples, final analysis of selected extracts, relating back of the analysis to the research question and literature, producing a scholarly report of the analysis.

The analysis has been conducted with our theoretical framework and research questions as the basis. In the analysis of the collected data, we followed all the phases of Braun & Clarke's (2006) thematic analysis, as presented in Figure 4.1. In phase 1, we transcribed and thoroughly read through all the data to get a comprehensive overview. In phase 2, we systematically coded the data, with each of the authors' individual coding on each transcript, resulting in a total of 165 codes between the authors. The codes were compared, grouped, and merged, and redundant or irrelevant codes were removed. This process was done in three iterations, resulting in 19 code groups and a significant lower code count from the original 165 codes. In phase 3, the codes were collated into potential themes, with 18 candidate themes identified. Out of these 18 themes, some were pre-assigned based on the model of Blind et al. (2017) and the framework of Martin et al. (2019). The codes were reviewed against these themes, and additional themes were made for codes not fitting into the pre-made themes. Including themes that are outside the scope of theory and not discarding these parts of the findings is essential, as being overly guided and driven by theory and theory alone can result in important findings not being identified, thus harming the study as a whole (Braun and Clarke, 2006). In phase 4, the themes were reviewed in relation to the coded extracts and making the initial thematic map. The defining and final naming of themes was conducted in phase 5, resulting in six overarching themes, with six sub-themes and the final thematic map,

presented in Figure 6.2. Finally, phase 6 is the presentation of the analysis and results in Chapter 6.

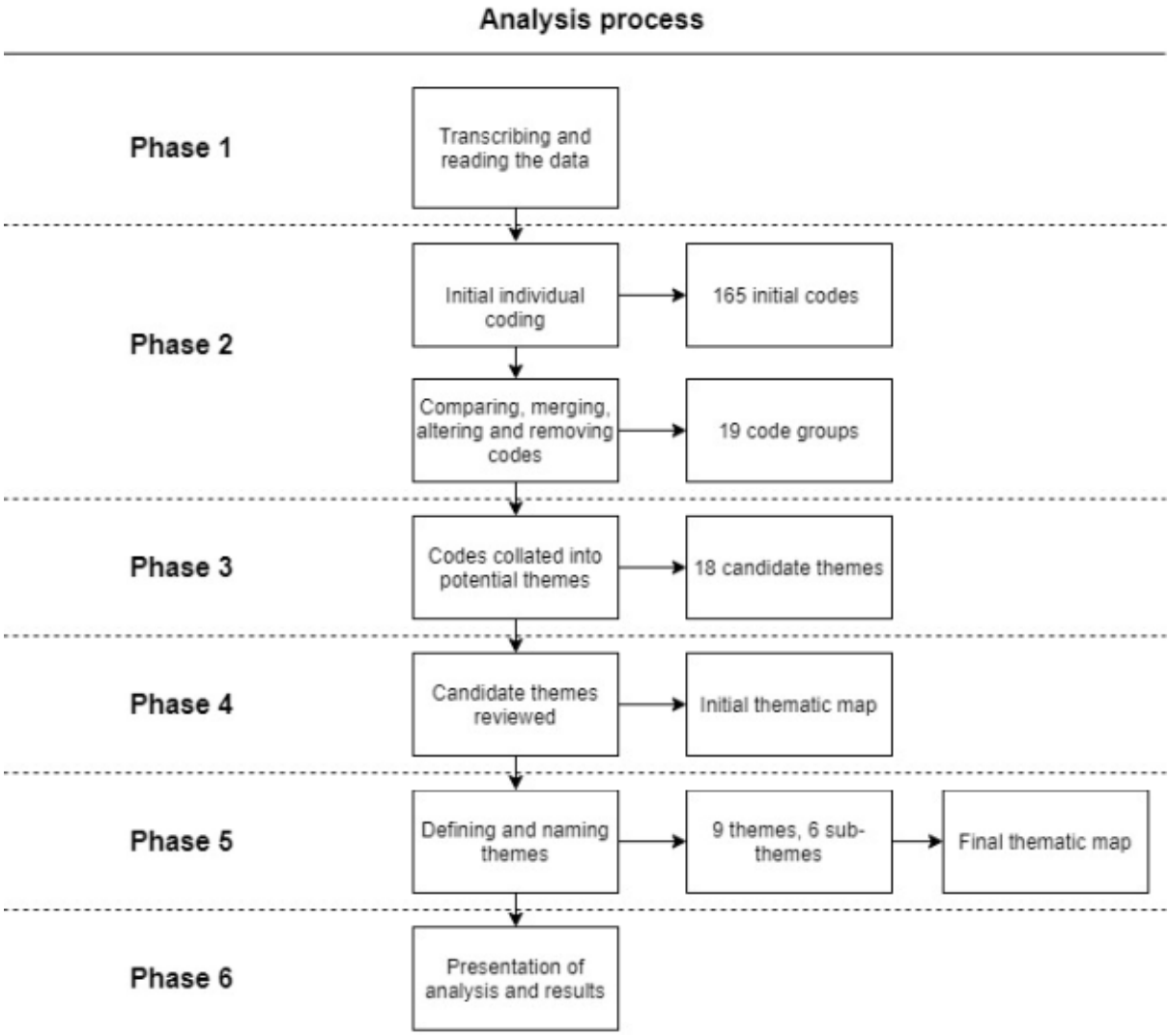


Figure 4.1. Thesis analysis process, showing the six phases of thematic analysis.

4.3.2 Analysis tools

For the analysis of this study, the tool NVIVO version 12 was used. NVIVO is a software that provides rich functionality to analyse qualitative data, where one can import documents and transcripts to be encoded, interpreted, visualised, and queried. One can co-operate on the analysis among several researchers, and the software provides a rapid, detailed, and straightforward way of extracting meaning from the data corpus and datasets (Qsrinternational, 2020).

4.4 Validity and limitations

For qualitative studies, validity is considered in regard to the suitability of the chosen processes, tools and data. For this study, the interviewees and context under which the data is collected align with the research questions this study aims to answer. Using a thematic analysis is appropriate and in line with an interpretive and exploratory approach to qualitative data. Further, triangulation has been applied to enhance the validity of this study (Leung, 2015). Investigator triangulation is the participation of two or more researchers providing different perspectives, and confirmation of findings, enriching conclusions. This master thesis is conducted by two researchers. The theoretical framework used in the analysis of this study combines the theoretical concepts of regulation and standardisation with privacy regulation on innovation, to assist in support of or to refute findings (Carter, Bryant-Lukosius, DiCenso, Blythe & Neville, 2014, p. 545).

As the interviews in the majority of the cases were conducted at the interviewee's workplace, one might consider the possibility of the interviewee being affected by the fact that co-workers and management know that an interview discussing different aspects of the company are being conducted.

The interviewees have been selected on geographical convenience to comply with the required date for delivery of the master thesis. A consequence of this might be that geographical differences in the specific domain may be limited. In total, 39 initial emails with a request for an interview were sent to candidates we saw as suited for the master thesis, with further second and third invitations by email/phone to those who did not respond. The response rate was low so we might have missed potentially good candidates with specialised knowledge in the domain. In addition, the Covid-19 pandemic was a factor for us when scheduling interviews in March and April. Potential candidates have declined our invitation for an interview due to prioritisation of Covid-19 related matters. The pandemic also had an impact on how some of the interviews were conducted. To comply with the Norwegian regulation on social distancing during the pandemic, interviews scheduled to happen on location and in-person had to be changed to video-interviews. While video-interviews work well in most cases, the setting and flow of the interview will not be the same as an interview in person. Aspects such as tone and body language might be more convoluted and difficult to recognise or interpret. However, the conducted interviews yielded saturated results for each research question, and so we find that the interviewed organisations and people to be sufficient for this exploratory study.

Since this master thesis exploits a qualitative research design, naturally, there will be ambiguities that are inherent in human language (Ochieng, 2009). A word that could signify different things might be misinterpreted in the analysis. Furthermore, a general limitation with the selected research approach to corpus analysis is that the findings cannot be extended to a larger population, segments, or domain with the same degree of certainty compared to quantitative analysis. This is due to the inability to test the data to discover whether they are statistically significant or due to chance (Ochieng, 2009). The conclusions of this study may, therefore, be more tentative than in a qualitative study, as the interpretation of the data is more closely tied to us as researchers, based on our identity, background, beliefs and assumptions. However, this form of study opens for more vibrant and detailed results, not reducing the results to numbers. Additionally, there is the possibility of alternative explanations and the acknowledgement that there is no one correct explanation. The study seeks the experiences and views of the informants, their reality combined with the interpretation of the researchers conducting this research, accepting that there is no single truth, and there may be multiple interpretations (Oates, 2006, p. 277).

4.5 Ethical considerations

There are ethical considerations related to conducting this study. While the people interviewed in this study are referred to as interviewees, they are humans and should be treated with respect and dignity. They should, wherever possible, gain some benefit from the research. In this study, that benefit is the outcome of the conducted research; that is the results and the discussion of the theory and literature towards the results, along with the conclusions. It is essential also to maintain the rights of the interviewees and interviewee candidates. In this study, each interviewee candidate has been given a consent and information form, explaining the purpose and context of the research, as well as the rights of the interviewees. This document is based on a template from NSD. The document clearly states the interviewees' rights not to participate, to withdraw, give informed consent, anonymity, and confidentiality (Oates, 2006, p. 54-59). A copy of parts of the study, where applicable, was also provided to the interviewees prior to delivery of the thesis, for the interviewees to review that no personal information is present in our master thesis in violation with the consent given.

We have also strived not to intrude unnecessarily. This entails not asking questions we do not need answers to and attempting to find available information on the topic and conduct a sound literature review before engaging in the interview process. It is important to behave with integrity, which entails recording data accurately and fully, not hiding or disregarding any data or results, even though it might hurt initial assumptions and theory. The collection, storing, access to, and destruction of collected raw data has been approved by the NSD to not conflict with the law and research ethics. The interviews have been recorded on an approved dictaphone, and the memory chip destroyed by the end of the project. Access to the data has been constricted to the authors and supervisors of this master thesis, in compliance with an approved procedure by NSD and information to the interviewees. Regardless of the interviews being conducted in person, by phone or digital solutions, recordings have only been done with the dictaphone, and no other software or technical device. During this study, it has also been of utmost importance to ensure that plagiarism and self-plagiarism do not occur (Oates, 2006, p. 60-63).

The data collected is to be used only for the purpose of this master thesis study and will not be shared or used for other research projects or purposes. Personal information about the interviewees is destroyed by the end of this master thesis study. The ethical considerations and decisions made for this study have been with a deontological approach, where the rights of the individual, such as data privacy cannot be overridden, even though it would benefit the domain and community where this study has been conducted. The main purpose of this study is to contribute to the field and theory, and not just to pass the grade of the study program this master thesis is a part of (Oates, 2006, p. 63-69).

5. Research context

This study is conducted in the south-east and central part of Norway. Interviews are conducted with public and private sector actors within the Norwegian health sector, with knowledge of HIS innovation projects and the General Data Protection Regulation.

5.1 Organisation of the Norwegian healthcare sector

At the top level, Norway is a constitutional monarchy, with the king as the head of state. In Norway, the power is shared between the government, parliament, and courts. The government contains the prime minister's office and the underlying ministries that serve the government (Regjeringen, 2019). In the context of healthcare, the Ministry of Health and Care Services has the top responsibility for health services, policies, and health legislation (Regjeringen, n.d., a). The Ministry of Health and Care Services is made up of eleven agencies and owns six enterprises. See Table 5.1 for the organisation of the Ministry of Health and Care Services.

Table 5.1. Organisation of the Ministry of Health and Care Services

The Ministry of Health and Care Services	
Agency	**Description**
Norwegian Directorate of Health	Monitor conditions that affect living conditions and public health, as well as trends within care and health services: advice and guides government, health enterprises, the private sector, voluntary organisations, and the population. Applies and interprets laws and regulations in the health sector and implements approved policies (Regjeringen, n.d., b).
The State Investigative Commission for Health and Care Services (UKOM)	Investigates serious incidents in health and care services. Collects knowledge about the incidents to make health and care services safer and better for patients, and discover the cause of the incidents (Regjeringen, n.d., a)
Norwegian Board of Health Supervision	The chief supervisory authority with overall professional supervision of health and care services (Regjeringen, n.d., a)
The Norwegian Institute of Public Health	Knowledge producer for the health sector, with tasks within advisory and services, method evaluation, health analysis, research and knowledge summary (Regjeringen, n.d., c).
The Directorate for e-Health	A driving force in the development of digital services in the health and care sector and has the national authority and the role of giving premises within the area of e-Health (Regjeringen, n.d., a).
National health service appeal body	Processes complaints in the health and care sector (Regjeringen, n.d., a).

Norwegian patient injury compensation	Processes compensation claims from patients injured by treatment failure in public and private health services (Regjeringen, n.d., a).
Biotechnology council	Consults Norwegian authorities in modern biotechnology matters (Regjeringen, n.d., a).
The Norwegian Medicines Agency	Supervision of drug testing, turnover and production (Regjeringen, n.d., a).
Directorate of Radiation Protection and Nuclear Safety	Professional authority on nuclear safety and radiation (Regjeringen, n.d., a).
The Norwegian Food Safety Authority	Supervision of plants, animals and food (Regjeringen, n.d., a).

The Ministry of Health and Care Services owns four regional health enterprises with overall responsibility for the special health services, somatic and psychiatric hospitals, ambulance service and other institutions, such as policlinics and treatment and rehabilitation centres. The regional health enterprises are Helse Sør-Øst, Helse Midt-Norge, Helse Nord, and Helse Vest. They also own the wholly state-owned corporation Vinmonopolet, with the all rights reserved task of responsibly selling alcohol like liquor, wine, and strong beer. The final enterprise is Norsk Helsenett SF, working within the framework of Norwegian ICT policy, maintaining national interests with operations and development of ICT infrastructure in the health and care sector, and striving for cost-efficient and safe electronic interaction (Regjeringen, n.d., a). In addition, the health sector has several state-approved private healthcare providers, and within ICT and IS, the public authorities and enterprises within health is working with national and international private sector ICT and IS providers (Helsenorge, n.d; Direktoratet for e-Helse, 2017).

5.2 The General Data Protection Regulation and Norway

Norway is not a member of the European Union, but has implemented GDPR as part of the European Economic Area (EEA) Agreement, an agreement between the EU member states and three of the four European Free Trade Association (EFTA) states; Norway, Liechtenstein, Iceland (Efta, n.d). Norway passed a new law for the processing of personal data (Personopplysningsloven) June 15th, 2018, and the law came into force on July 20th, 2018. The law conducts the GDPR, and thus makes the GDPR Norwegian law. The Norwegian law contains what is necessary to fulfil the GDPR and supplements the parts that the GDPR leaves for each country to create national rules (Regjeringen, 2019). The geographical scope of the law applies to the treatment of personal information in connection to the activities of data controllers and processors in Norway, regardless of the treatment being done within the EEA or not. The law also applies to data processors not established in Norway but established in a place where Norwegian law applies under international law, and of the treatment of personal information on registered persons located in Norway handled by data controllers or processors not located in Norway (Personopplysningsloven, 2018, §4). The law continues the essence of the expired former law and Directive 95/46, with the GDPR as the main basis (Regjeringen, 2019).

5.2.1 GDPR and the Norwegian health sector

The privacy protection and information security laws in Norway were strict prior to the GDPR. However, the GDPR has presented some changes to the laws and practices. GDPR inflicts a stricter requirement for consent as a legal basis, and special care is taken if there are

children involved. For consent, it must now be as easy to withdraw consent as it is to give consent, consent must be unequivocal. When it comes to consent for receiving healthcare, Norwegian law accepts consent in the form of conclusive behaviour, and health personnel must register information in a journal, and the documentation requirement is the legal basis for the treatment of personal information. It is thus deemed that no further consent requirements are needed. The patient can, however, withdraw this consent, and the patient should be notified of the consequences this implies. The arrangement of concession and notification to the Norwegian Datatilsynet is now void, and thus one does not have to apply to Datatilsynet to process personal information (Direktoratet for e-Helse, 2019a). The Norwegian Personopplysningsloven, with its foundation in GDPR, has several laws concerning personal information in the context of health and care in Norway, and Normen tries to sum up and inform on the important areas in regards to GDPR and health and care, as well as other Norwegian laws concerning personal information and information security in the context of health and care (Direktoratet for e-Helse, 2020a).

5.2.2 Normen

The Norwegian health and care authorities, in collaboration with actors in the Norwegian health and care sector, have since 2006 developed and revised an industry norm that can be followed in the Norwegian health and care sector.
The norm for information security and privacy in the health and care sector (Norwegian: Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren), also commonly referred to as Normen, is an industry norm that contributes to satisfying information security and privacy considerations in infrastructure, common systems, and enterprises across the Norwegian health sector. Normen is continuously improved, with the latest version, version 6.0, adopted February 4^{th,} 2020, and applied from February 5^{th,} 2020. Normen applies to any enterprise that has committed to follow Normen. Normen is presented as to be used as a guide and a tool, and the requirements listed in Normen have two priorities, requirements that must be met, and applies to all actors, and requirements that should be met, where it is for the actors to consider and decide upon applicability. Normen has the basic purpose of contributing to good privacy protection, education of health personnel, ensuring quality, patient safety, health services, and patient health services. Normen covers many Norwegian laws that affect information security and privacy protection in the Norwegian healthcare sector, but not every aspect and law with affiliation to information security and protection of privacy. Normen is compiled and managed by a management group from the healthcare sector, with permanent participation from Norwegian Health Net SF, and the Directorate for e-Health is the management group's secretariat. Additionally, several enterprises and actors from the healthcare sector are involved in the preparation of Normen (Direktoratet for e-Helse, 2020a, p. 8-10).

Normen includes an appendix, *Samlet oversikt Normens krav*. It is an overall overview of Normen’s requirements that must be met, with a checklist to check if a requirement is met or not. It is intended to give a systematic overview of Normen’s requirements, and as a tool for conducting safety audits for procurements, suppliers to document compliance or system development. Both Normen and the overview of Normen’s requirements focus on four main topics; Management and responsibility, risk management, basic treatment of health and personal information, and information security (Direktoratet for e-Helse, 2020c). A smaller version of Normen and the requirements list is also developed, aimed at small enterprises and sole proprietorship (Direktoratet for e-Helse, 2019b).

6. Analysis and results

In this chapter, we present the analysis and the corresponding result of the data collected through this study. The empirical data is initially collected in Norwegian, but the citations have been translated to English in this document. First, the outcome of the analysis is presented in the form of a thematic map (see Figure 6.1). Further, the analysis results are presented based on the structure of the thematic map, presenting the results for each overarching and connected sub-theme. Finally, we sum up the results.

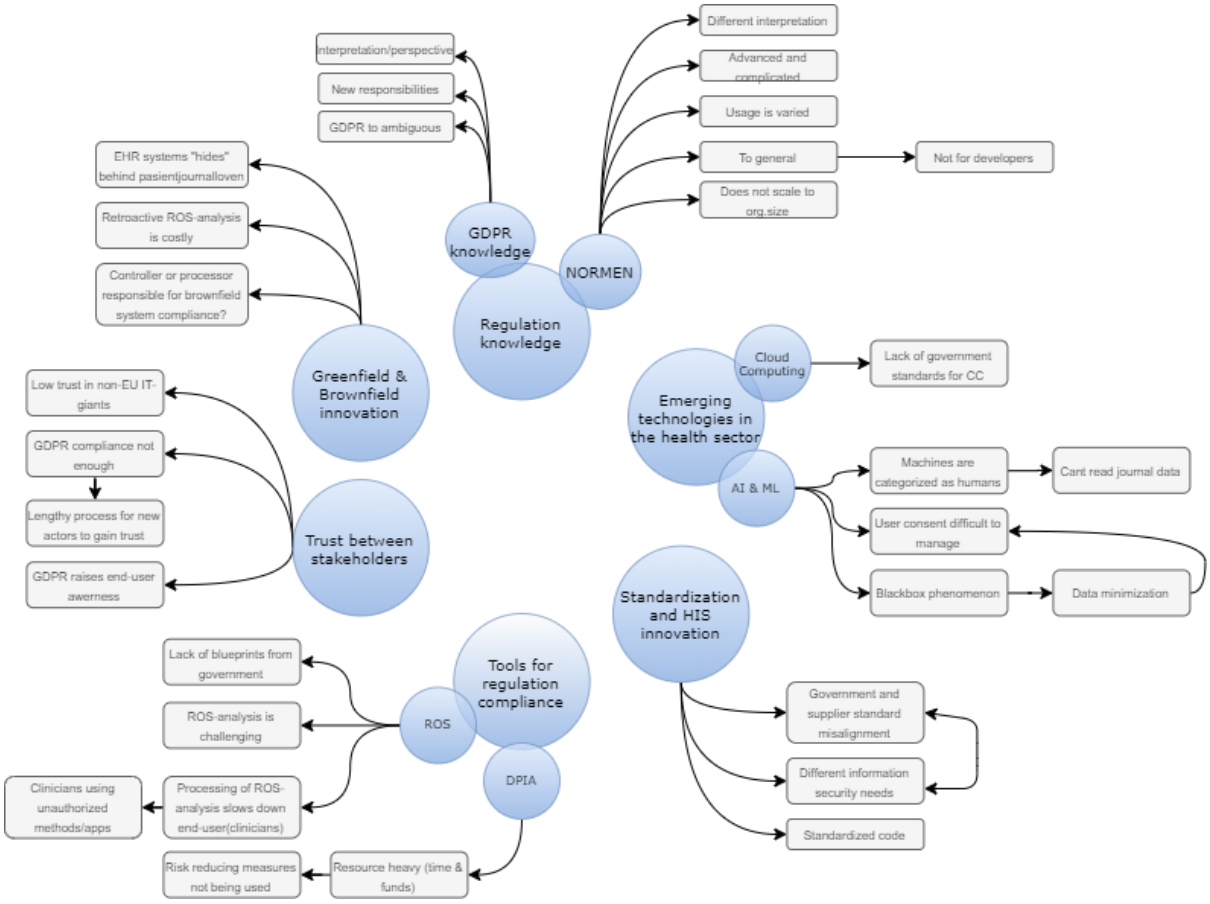


Figure 6.1. Thematic map based on the results of the analysis

6.1 Knowledge on regulation

The GPDR has been interpreted differently amongst actors in the healthcare sector and there is a lack of knowledge on the regulation. The GDPR is complex and big, giving leeway for organisations themselves to assess and evaluate if HIS innovations are compliant with the regulation. Normen, the tool summing up relevant information security, health and privacy legislature made for the Norwegian health sector is also vast and comprehensive. Educating staff on privacy regulation is important, and actors seem to have different knowledge level of the regulation, with additional different interpretations of the regulation causing negative effects on HIS innovation.

6.1.1 Knowledge on the GDPR

One of the aspects touched upon in our interviews was the interviewees' experiences and feeling connected to education and knowledge on the General Data Protection Regulation. Out of a total nine interviewees, seven of them expressed that there is a lack of knowledge connected to the GDPR.

Common to the majority of conducted interviews is that the General Data Protection Regulation is a comprehensive and extensive regulation to adjust their innovation and organisation around. *«GDPR is so big and comprehensive, so the primary challenge is to have a good enough grasp and knowledge on it. Be aware of what risk you are taking, and thus can more easily take that risk. »* (Interviewee 1). We identified consensus among interviewees that the regulation is imposed on organisations with good intention and for the benefit of consumers. The principles in the regulation are reasonable, but the regulation, in theory, is different from the regulation in practical terms.

> *«The principles in the regulation are, in fact, very reasonable and easy to work with. It is the practical use of it that is intricate and difficult. But, I believe that in a couple of years, when we have gotten the regulation under our skin, it will settle. »* (Interviewee 9, personal communication).

GDPR has not only set in motion limits and barriers for what organisations can do with personal data, but it has also indirectly put a new burden on actors processing personal data in the way that they internally have to discuss privacy matters and raise the general awareness connected to the regulation. GDPR also incorporates the fact that organisations must educate their staff. The organisations' management must get an overview of what needs to be educated, produce material, develop education programs, and endorse wanted behaviour. Furthermore, another interviewee expressed the importance of educating managers and leaders. Interviewee 8 tells us that they have had a significant focus on expanding their organisations' knowledge on the regulation. This has increased their ability to acquire compliant systems from suppliers, but also the ability to expose weaknesses in systems and point them out for the supplier for patching or replacement. Interviewee 2 expressed these aspects in the following quote:

> *«Leaders are the all-knowing oracles in organisations. The workers will go ask their leaders before they even bother looking up their issue or problem in the documentation. You can't put all effort into educating the workers; you have to raise the knowledge and awareness of management and leaders. »* (Interviewee 2, personal communication).

The education of management and not only the workers can be identified as a key factor for understanding and successfully implementing GDPR in several of the interviews.

«One of the most important things I have witnessed that might have been lacking in other projects is the fact that our decision-makers always have GDPR in the back of their head. One should not underestimate the importance of decision-makers ability to estimate risk based on privacy and information security. » (Interviewee 4, personal communication).

Due to different levels of regulation and a varied interpretation of GDPR, management and clinicians at a Norwegian hospital experienced conflict connected to information security and beneficial health services. The management has the responsibility for the patients and patient security. They advocate a very strict interpretation of the regulation regarding privacy. On the other hand, doctors are expressing that privacy regulation is in the way of patient treatment and patient security. The interviewee says that situations like these create endless discussions since the different actors do not "speak" the same language.

« There is a potential solution to everything, but when even privacy lawyers and Data Protection Officers do not know how we are supposed to handle and interpret GDPR and are frightened to make mistakes… It makes the process of getting innovation to production very long. » (Interviewee 7, personal communication).

A reoccurring theme is that HIS received from a supplier has glaring shortcomings regarding standards, modules or functions connected to privacy. It is not clear if this stems from lack of knowledge of the regulation or if HIS suppliers have a different interpretation on GDPR.

«We now have the competence to identify shortcomings or missing features in systems provided by a supplier and give feedback for needed fixes for the solutions. In many cases, we have seen quite glaring shortcomings with many different suppliers: missing two-factor-authentication, secure login and modules for delete routines to name a few. We have pointed out several things that need fixing for the solutions to be GDPR compliant. » (Interviewee 8, personal communication).

There is a combination of uncertainty and lack of knowledge and a very bureaucratic approach to how privacy regulation should be interpreted. There is a lack of a unified interpretation of GDPR in general. Regarding the interpretation of GDPR, there have been identified two main views of how this affects HIS innovation. The first is how a strict interpretation of the regulation is in the way of innovation and stops potential HIS innovation initiatives that could make the healthcare sector provide better and more effective healthcare. *«Doctors at the big hospitals in Oslo stated that the strict interpretation of GDPR had killed more people than it has stopped their personal data from leaking.»* (Interviewee 7, personal communication). The second view is a more positive take on what effect GDPR has had on HIS innovation. One aspect is that GDPR has given more room for interpretation for innovators and project leaders. While GDPR has strengthened the penalties for breaking the law, it has eased up some of the very technical specific limitations formerly put on innovation. This gives the innovators and project leader greater leeway when deciding if the innovation is within acceptable parameters.

«GDPR has massively increased the penalties for breaking the privacy law. We have already a privacy law from earlier that are very technical specific with limitations. With the implementation of GDPR it has created a bigger leeway and to some extent taken away some of the very specific formulated principles which have resulted in us being able to make assessments ourself and evaluate if privacy is protected sufficiently. » (Interviewee *2*, personal communication)

In addition, there is a view that GDPR creates challenges that need to be overcome and a result of this is that GDPR is a driver for new innovative solutions.

GDPR brings with it the need for a more transparent relationship with end-users' data. Involvement of citizens and individuals and making privacy data available gives new arenas for innovative user-centric solutions that can make people's daily life easier.

> *«I see GDPR as an enabler for innovation since involving citizens or individuals.., especially in health… making available information for individuals gives the possibility to innovate many new services. Giving individuals the right to choose who can access his personal information creates the possibilities for new services that covers his needs to be developed.»* (Interviewee 5, personal communication).

See Table 6.1 for an overview of the theme results.

Table 6.1. Knowledge on the GDPR and implications with respect to innovation.

Finding from analysis	Result implications	Effect on innovation
Actors have a different interpretation and perspective on GDPR	Creates problematic situations in the organisation when management and staff are not on the same level regarding how they should interpret the regulation. In health, there is also a clear concern from doctors who states that GDPR is in the way for patient safety and treatment.	Potential novel health initiatives that could improve health services are stopped based on innovator not having the sufficient knowledge to make the innovation GDPR compliant, or that management is overinterpreting the regulation and therefore stops the innovation.
Regular staff and management staff gets new responsibilities with GDPR	With new responsibilities, greater focus and resources have been introduced for education on the regulation.	1. This will put additional strains on innovators, who have to redirect focus away from the innovation and over to privacy law. 2. With the newly acquired knowledge of GDPR, management can make a better evaluation to check if innovations are meeting standards set by the regulation.

GDPR is ambiguous	GDPR comes with big fines and penalties when a law is broken, but due to its ambiguous nature, it also gives innovators bigger leeway and has removed very specific technical limitations previous law had.	1. With innovators more in charge of assessing risk connected to their innovation, it is more likely that the innovation can move further in the development cycle. 2. Startups need specialised advisors or special knowledge connected to GDPR when innovating new health systems. The risk of fines and punishment for non-compliant innovation might deter innovators with novel health innovations from pursuing them.
GDPR is comprehensive and complicated	While the principles of GDPR is reasonable and easy to work around, the practical use of it is intricate and difficult. Challenges connected to have a big enough grasp on the regulation and knowledge about it arises.	While innovators are compliant and follow all aspects of the regulations on paper, in practice, the innovation is "strangled" by all the limitations set by the regulation.

6.1.2 Challenges with Normen

Normen was one of the topics that our interviewees spent the most time talking about their thoughts and experiences. Several implications or effects on innovation were identified connected to Normen. When coding and categorizing the interviewees, we discovered a distinct divide in positive and negative attitudes and experiences towards Normen. The first significant finding was how Normen is comprehensive and does not differentiate on the size of organisations. Firstly, there are several of the interviewees that point out that Normen is too general and is not fit for use in smaller health institutions. It is developed with large health institutions in mind and can be very troublesome for more minor actors to handle and be compliant.
When working with the *NORM* for information security in the health sector, the issue can be seen Interviewee 2 stated.

> *«When working with Normen, there is a lot of actors involved. There are management groups and reference groups and a lot of paperwork. It involves suppliers and Helse SørØst, who are a big and heavy actor. But it also includes small actors as the medical association that represent different general practitioners. And of course, they see the obvious problem that they are subject to the same strict regulations».* (Interviewee 2, personal communication).

Interviewees 4 and 9 had similar thoughts on the matter and mediated the same message through their interviews when asked what potential weaknesses Normen have.

> *«Other private health institution such as GP offices and physiotherapists feels that Normen is way too comprehensive and complicated. They think that Normen is more*

> *customized for big organisations such as hospitals that have resources at hand».* (Interviewee 9, personal communication).

> *«With the arrival of Normen v.6.0, Normen is now covering requirements in the GDPR while it also is technology-neutral and is adapted to today's technologies. While there are many strengths to Normen regarding information security, it also has a great weakness; It is supposed to govern all actors within healthcare. Normen should equally be the framework to follow for a big health institution, as well as small actors such as a tiny GP office».* (Interviewee 4, personal communication).

Interviewee 5 stated that Normen is facilitated for management level and not for development. Normen should be more specific for different types of audiences. *«I experience that when we try to implement Normen's guidelines into how our developers develop, they easily get confused and ask; what does this mean for my work?»* (Interviewee 5, personal communication). Secondly, there were other barriers connected to Normen and how it implicates how organisations use it. Normen as a tool has good intentions, but often, it is the interpretations of it that will complicate things. Interviewee 7 stated that the public sector would greatly benefit from raising its competence regarding use of Normen. Interviewee 7 also said that it is not directly GDPR, but approvals connected to Normen that often spell death for many innovative processes. In addition, interviewee 7 explains how there is a discrepancy between what Normen and GDPR say about how data should be processed and registered.

One of the main goals when revising Normen to version 6.0 was to simplify the presentations and to make Normen more reader and user-friendly (Direktoratet for E-Helse, 2020b). In the conducted interviews, it is revealed that there is still an issue with how it could be difficult to understand and get a grasp of Normen.

> *«We have been going through training and courses connected to Normen, but the practical use of it and overview of Normen I think is still very difficult».* (Interviewee 8, personal communication).

> *«It is a very comprehensive and complex industry-norm that is not very easy to get a total grasp on. Normen is structured for the different implementation level you are using it for, but it is very comprehensive and has big checklists that can tire you out pretty easily».* (Interviewee 5, personal communication).

While there was a consensus that there are some problematic areas of Normen, the interviewees also shared several positive experiences. When developing their management system for information security, in many ways, it includes Normen Interviewee 4 said. They got much inspiration from Normen and used it in some way as a blueprint for their system. Normen is described as a great tool to use when working with information security. Normen summarizes current legislation and gives simple recipes on how you could go forward with a project or implementation and still be compliant.

> *«We use Normen as the main rule or rule-of-thumb. If Normen says it is not okay, we will not move forward with our initial plan. If Normen says it is okay, we use that as approval for our project. We appreciate Normen for what it is».* (Interviewee 9, personal communication).

As seen earlier in this chapter, some interviewees expressed that Normen can be challenging to use and interpret. On the contrary, Interviewee 7 was outspoken on thoughts about Normen, and how it is pretty straight forward. Interviewee 7 said that while it gives some limitations to a pragmatic approach, it sets clear and reasonable boundaries for them to work within. The purpose is to secure information security and privacy and handle sensitive information, and that should be seen as a good thing.

Some interviewees described Normen as challenging to use for smaller health institutions based on Normen being developed with big health institutions in mind. Interviewee 4 had a different experience and thought Normen should be seen as an excellent resource for smaller actors. *«I think Normen does an excellent job to exemplify how you can do it. In addition, I think Normen is a big resource for smaller actors within the health domain»*. (Interviewee 4, personal communication).

See Table 6.2 for an overview of the theme results.

Table 6.2. Results of analysis for challenges with Normen

Finding from analysis	Result implications	Effect on innovation
Comprehensive and does not differentiate on size of the organisations	Smaller actors such as physiotherapists and GP's have to understand, comply and work around the same guidelines as big actors such as hospitals	Stifles the possibility for small innovative ideas to flourish as more minor actors might not have the resources at hand to make innovation comply to Normen
The discrepancy between GDPR and Normen regarding the processing and storing of data	Creates confusion in legislation on what is the dominant law	How does the owner of innovation comply to if Normen and GDPR have different guidelines on being compliant?
Normen still challenging to understand and get a total grasp on(post 6.0)	Personnel need extensive training and courses. A large checklist that can be overwhelming and tiresome	Problematic for innovators without vast resources to be educated enough to make innovation comply to Normen
Normen meant for management, not developers	Developers have a hard time understanding what implication Normen has for their work, and how they should comply with guidelines	Developers develop solutions that are novel but not compliant towards Normen.
Normen as a blueprint for system development	Will simplify building solutions from scratch as the guidelines in Normen sets clear boundaries	Shortens the development time of innovation since Normen operate as an industry standard that gives clear guidance on how data should be stored and processed.
Summarizes current legislation	Makes legislation more accessible and simplify advanced wording and context	Innovators have easier access to an industry-standard that is not convoluted and hard to understand. Makes development of innovations without significant juridical resources possible.

6.2 Emerging technologies in the health sector

The GDPR, in combination with local health regulation, has affected emerging technologies in the healthcare sector, such as Cloud Computing, especially foreign public cloud solutions, and ML, natural language processing, and AI.

6.2.1 Cloud computing

GDPR and local privacy and health regulation impact the use of cloud solutions in the Norwegian health sector, because of strict regulatory enforcement of privacy regulation within public hospitals and a looser interpretation and enforcement in the municipalities and primary healthcare in local communities. Cloud computing is being used as a platform for HIS in the public sector but on different levels. Within primary healthcare in the local communities, cloud solutions are being used as a platform for data storage and applications. Public hospitals, on the other side, do, in general, not accept public cloud solutions due to the data being stored abroad or the lack of data control that comes with public cloud solutions. Interviewee 1, 2, 6 and 7 talks about cloud computing as a "no-go" option for public hospitals, as they need to have total control over the data, and have the data within national borders.

> *«If you look at the history of hospitals, they are traditional and slow, and all the data they have are stored in their own basement, their own data centres, public cloud solutions is something they fear and do not relate to. End of story. Everything that happens beyond their control area is not secure, and thus by definition, something they do not want to use. »* (Interviewee 2, personal communication).

Using external cloud solutions for HIS in hospitals is challenging, as the hospitals as data controllers have very strict enforcement of GDPR and local privacy law, thus finding external cloud providers as data processors, especially outside of Norway, not compliant enough to process the data. Hospitals feel they lose the required control over data that the regulation demands when using external providers, especially towards control over unauthorized access.

> *«Using foreign cloud providers is, in general, not okay. You can have agreements and contracts in place with cloud providers, but you do not have total control over the data, and hospitals feel they need control down to a very deep level. How can you know that there are not unfaithful people in the basement of a cloud provider with physical access to data? And because the data is personal information, it can identify people, and because of this, you are required to comply with GDPR. It does not help that the data is just a simple code somewhere. So innovation initiatives that contain something outside the hospitals own control area is challenging.»* (Interviewee 2, personal communication).

The strict interpretation of GDPR in combination with local health regulation is hence seemingly experienced as a barrier for cloud computing-based HIS innovation for use in hospitals and slows down HIS innovation. The strict interpretation and refusal to use foreign-based cloud services is however experienced to be constricted within the general regulation interpretations in Norway, and interviewee 7 experiences that this is not the case in the rest of Europe:

> *«Some of the Norwegian lawyers, data protection officers, and information security leaders point to great difficulties when it comes to legally pursuing a potential court trial outside of Norwegian borders. This is, however, not the case in the rest of Europe. It is only a case in Norway, as Norway is the only country with such a strict interpretation of GDPR. »* (Interviewee 7, personal communication).

External cloud providers are, however, used by municipalities within primary healthcare in local communities. It is recommended not to store data locally and instead use external cloud solutions according to interviewee 8. Cloud solutions and agreements with cloud providers

are frequently used according to interviewees 3, 7, 8, and 9. Cloud solutions are, however, not unheard of in a hospital setting. Such is the case for a project implemented with breathing machines, interviewee 2 explains. The patient is given a breathing machine from a hospital to use at home. These machines are used by 6000 patients and come with a GSM modem, that can be turned on or off. When turned on, the data is sent to the provider's cloud in France, and the settings can be adjusted remotely. The machine identification number is coded in internal lists at the hospital with a connection to patient information. Thence it can be used to identify the individual patient along with the stored health data from the machine. If the GSM modem is turned off, issues with the machine must be fixed on-site in a hospital, using the patient's and doctor's time. Additionally, if there are wrong settings or faults with the machine, the patient must use it with faults or wrong settings until the doctor can read the data and tweak the settings, usually once a month. There is enough argument to make use of the original software and store the data in France, but there are still some concerns interviewee 2 explains:

> *«There is always some form of a Facebook group for "us who use this and this brand", and the patients find each other. And of course, the supplier provides an application where you have access to the data, and you can register with full name and address and everything. So firstly, you enrich the data in the datacenters in France, so what used to be just a code that was hard to use to get information about who the person is, now is fully identifiable information, the patient says "This is in my interest, and I want this to happen because the application gives me full coaching and by doing this I get a better user experience". They do not think about the responsibilities the hospitals have when it comes to taking care of the data, and that the data now is indirectly compromised.»* (Interviewee 2, personal communication).

Concerns arise when the registered patients themselves expose their data, compromising the privacy security measures the hospitals have ensured to be in place. Interviewee 2 further calls for a formal standard for cloud solutions in a hospital setting, thereby making it easier for innovative HIS entrepreneurs to enter the health and care sector and innovate with cloud-based solutions. There seems to be no collective agreement in the public health sector on how to handle external cloud-based providers. Consequently, the use of such services varies greatly amongst public sector health enterprises.

See Table 6.3 for an overview of the theme results.

Table 6.3. Results of analysis for cloud computing

Finding from analysis	Result implications	Effect on innovation
Public hospitals have a strict interpretation of privacy regulation	Public hospitals generally do not accept and implement external cloud-based HIS innovations due to them loosing too much control over the data	External cloud-based HIS innovation is generally not adopted by hospitals, slowing down and in worst case stopping innovation possibilities and discouraging entrepreneurs
Cloud-based HIS solutions will greatly benefit the efficiency and quality of healthcare	The Norwegian hospitals see the potential cloud computing technologies offer, and want to find a solution to start adopting cloud-based HIS	Can open up possibilities for HIS innovation with cloud-based HIS in Norwegian hospitals
Difficult to legally pursuit a potential court trial outside of Norway due to Norway's strict interpretation of GDPR	Negatively impacts the decision to adopt and implement international cloud-based HIS innovations	A contributing factor to hospitals not adopting external cloud-based HIS innovations, thus slowing down or stopping innovation progress within cloud computing technologies in the health sector
Social media and innovators applications enable patients to bypass hospitals privacy security measures	Data is indirectly compromised, resulting in data controllers not having full control over patient data stored in public cloud solutions.	Privacy protecting efforts implemented for compliant HIS innovation is discarded by the users and cloud providers, making it hard to maintain a compliant system as a whole.
Municipalities and primary healthcare in local communities take advantage of cloud-based innovation for HIS, in contrast with hospitals	Evidence of different interpretation of GDPR or different regulatory enforcement in various areas of the healthcare sector	Novel health innovation that utilises or is dependent on CC as a technology cannot be scaled up to the national level. This limits the amount of use-cases for the innovation. Without potential scaling, the innovation can be deemed non-profitable by the innovator.

6.2.2 Machine learning and artificial intelligence

GDPR has had an effect on innovation of HIS in regard to ML and AI. The overall pattern is that issues with collecting consent when using large amounts of data are troublesome, and the technology is currently within the health sector predominantly at a research stage. To process data with AI, the vast amount of data needed to develop the algorithms makes it difficult to handle consent from individuals according to interviewee 1:

> *«Every document belongs to an individual, and the individual has unique rights in relation to GDPR, so you have to use that as a starting point. For instance, we need to ask for consent in advance from a patient to use patient data for research projects. That is troublesome when we are in this setting talking about millions of journal data.»* (Interviewee 1, personal communication).

HIS innovation often does not move on from a research project to full implementation in practice. The issue is that research projects often have a small scale, use fewer amounts of data, and are easy to approve for AI and use of data, as the data is often a sample or test data. When one puts this into normal operation and production, the ML algorithms run continuously, on large quantities of data. This creates issues, as you need a legal basis to access and process journal data. Only the ones with authority to access data for treatment purposes of individual patients can access the journal data. The issues then arise when trying to find a legal basis for a software program trying to access vast amounts of journal data. GDPR's negative effect on HIS innovations utilizing ML is expressed by interviewee 2, 3 and 5, where such projects are often limited to research projects or pilots.

All interviewees in this study express that the use of AI innovations in the health sector would greatly benefit healthcare, research and services provided to both clinicians and patients, and they are positive to explore this emerging technology in the health sector. The use of ML algorithms and AI is being used to some degree, mainly within IT security. Interviewee 4 explains that they are trying out AI to detect malicious content on their platform. As of now, the ML algorithms are developed, so they want to use normal behaviour as the starting point, so the AI can more easily detect abnormal behaviour. Interviewee 4 see the benefit to use AI to recognise what effect medical drugs have on the population, but that today's laws are a barrier to achieve this. It is also possible to accomplish some analysis with ML, for instance, the analysis of blood pressure. By using the principle of data minimisation, you can set up the algorithms to only use the data that are needed. Interviewee 7 explains that to do this kind of analysis, one does not always need to know whom the blood came from or in what context, you can set it in a meta-context, and make vectors where ML can contribute to predictive analysis. However, the principle of data minimisation also makes it hard to single out the actual data required to have the AI working as intended, while still being fully compliant with the law, collecting all required consent and have a legal basis for the AI's access to large amounts of health data.

See Table 6.4 for an overview of the theme results.

Table 6.4. GDPR with Machine learning & Artificial Intelligence

Finding from analysis	Result implications	Effect on innovation
Cannot collect consent from all patients when using large amounts of data for AI.	Without consent, it is troublesome to analyse big data in ML algorithms.	Slows down the innovation progress within the context of AI in HIS solutions.
Hard to have a legal basis for an AI to access large amounts of patient data.	A legal basis is needed to provide healthcare to individual patients by accessing journals. ML algorithms and AI software do not have a legal basis for accessing large amounts of patient data.	Without a legal basis, AI software remains at the earlier stages of the innovation process, as it cannot be deployed fully into production.
ML algorithms and AI software are seen as a positive contributor to raise healthcare quality.	Stakeholders within the healthcare sector are positive to explore the possibilities provided by AI.	Triggers innovation within healthcare AI, as innovators are looking for ways to develop regulation-compliant AI.
A lot of the AI innovation projects end up as pilot projects or research projects.	The need for consent, legal basis and data minimization principle acts as barriers for fully implementing AI innovations, resulting in many pilot projects or research projects that do not move on to production.	Many innovative ideas and tested solutions are stopped, halting the progress of innovation with AI solutions in the healthcare sector

6.3 Standardisation and HIS innovation

The results for the aspect of standardisation can be viewed in the context of *Strict regulatory enforcement*, as presented by Martin et al. (2019). The reasoning for this stems from the fact that the Norwegian health sector is positioned in this regulatory segment, and the Norwegian health legislation sets several parameters for which standards and norms Norwegian health sector follows.

The main finding regarding this aspect is that all our respondents express that the Norwegian health sector domain is not where it should be when it comes to standardisation. If each organisation and institution develops proprietary solutions which utilise its own standards, this will slow down the health sector's possibility to respond to incidents or a change in the national demographic. A solution to this issue is to build a platform based on standards that every actor can follow and be unified around. Citizens and patients expect to meet health services that are coordinated. One specific interview revealed that getting all actors onboard for a shared platformed with standards that everyone agrees on is one of the main hurdles to overcome today.

> *«The biggest challenge I see is that municipalities and hospitals all have proprietary solutions and do not cooperate with each other. There needs to be standardisation, so the sector has one platform to work on, especially when it comes to ICT and data, to get all actors onboard on the concept of one patient, one patient journal, one access point. »* (Interviewee 1, personal communication).

When we are talking with one of the interviewees, the conversation naturally flows over to the subject of standardisation connect to technology, specifically Cloud Computing**.** There is a need for an initiative that establishes a national health cloud service. If this becomes a reality, the health sector has more leverage towards suppliers when negotiating potential deals or partnership with suppliers.

> *«If we can establish a national health cloud service we could say; "hi suppliers, if you want to come and offer your systems or services here in Norway this is the standards your system must be compatible with and comply to". It has to be a national initiative, and somebody must put forward the money for it. We are in dire need for it. »* (Interviewee 2, personal communication).

While some of the Norwegian municipalities have been utilizing external cloud computing solutions for years, the hospitals have been more reserved, and it has been the ground for frustration and a call for a greater joint effort into creating a national health cloud solution. There was good progress in developing a cloud-based platform, that was supposed to function as a national test and development arena. It was named Medicloud and developed by Invent2 AS in partnership with Sykehuspartner HF. Its vision was to facilitate quicker health information technology-innovation and was a health-related cloud solution built upon open standards. Medicloud was meant to be a platform aimed at both developers and innovators, where they could easily test out their innovations on test data. This initiative was stopped in Q3 of 2017 due to barriers related to scaling, security and privacy (Øvrelid & Bygstad, 2016, p. 52-53). Issues revolving around hospitals' lack of utilization of cloud computing were expressed firmly:

> *«We have not even agreed on the criteria for safe use. We have not managed to be unified in how we should understand and control a partnership or collaboration with a cloud computing service provider.»* (Interviewee 2, personal communication).

Standardisation is vital for the health sector to advance, along with the progression of technology. One interviewee points to how thriving the telecom industry has been with their standardisation of 5G and IoT. This type of standardisation is needed in the health sector, but it demands extensive funding. *«The type of standardisation the telecom industry have seen is exactly what we need in the health sector. What is stopping us is not getting actors on the same page and a government who is indecisive. »* (Interviewee 5, personal communication). The strict interpretation of the regulation and lack of a compliant cloud solution that Norwegian hospitals can utilise created episodes where radiology images are physically sent with a taxi from one health institute to another. The lack of standards and the possibility to request access to information across health institutions journal systems have significant implications for Norwegian health sectors' efficiency. Norsk Helsenett SF(NHN) now runs projects that are set out to solve the matter at hand. With the establishment of a portal where health personnel can authenticate their identity, search, and render or stream data. This can be a potential solution for sharing data between health institutions but comes with a new challenge since standardisations are not unified across the whole health sector (i.e. private

clinics, pharmacies, general practitioners and hospitals). Interviewee 2 had this view on the new challenged connected to data sharing:

> *«They do not get free and uncontrolled access into our journal system, but they can apply for access to journal documents. The new dilemma that arises is how we should deal with our strict security measures connected to patients data and network security when someone requests access? There are GP's that are not regulated as strict as us or do not interpret the regulation as strict as us when it comes to information security and network security. »* (Interviewee 2).

The specific aspect of standardisation of health data was also something two of the interviewees had experiences with and they felt needed change or improvement if the Norwegian health sector was to be able to utilise, in particular, ML. Interviewee 7 who works for a private company, which delivers software for Norwegian health institutions, states that the challenge regarding privacy connected to personal data is solvable since their ML solutions manage data in compliance to laws and regulation. Still, they cannot use it because the Norwegian health sector lacks enough structured data. *«It is actually a "small data" problem. There is a lack of good enough structured data. So you could say "it is a big small data problem". »* (Interviewee 7). Regarding this issue, one of the interviewees who works for a private consulting firm said that they earlier looked upon GDPR as a potential solution to this problem. But in retrospect, the experience was that other specific health legislation guides and laws such as Normen and the patient journal law, in reality, override GDPR and still uphold this barrier.

> *«One can get a print of patient journal if you ask for it, but the data is in an unstructured form and not really useful for anything. Since its unstructured data, we cannot really combine it with other types of data to develop solutions that can be beneficial to health. »* (Interviewee 5).

There are also traces of steps being taken to reduce or eliminate this challenge. Interviewee 4, who works on privacy matters for a company who develops a national platform for a specific health institution segment, stated that standardised data is crucial in today's HIS.

> *«In our project, we have a big focus on the reuse of standard code. Standardisation of code is important, and we want to eliminate the use of free-text fields. This will contribute to the aspect of data minimization. If we do not have standardised information in today's technological solutions, what do we even need that information for? »* (Interviewee 4).

Interviewee 6 expressed that roles on standardisation as of today are not what they should be. As a worker in a private medical technology company, the interviewee explains that there is confusion on who should be responsible for establishing the standards. Explicitly, he endorses the idea of a procurer, or public sector, making a more significant effort in developing sustainable architecture and standards, and to a greater extent, leave the development of solutions that comply with said standards and principles to the market.

See Table 6.5 for an overview of the theme results.

Table 6.5. Results of analysis of standardisation and HIS innovation

Finding from analysis	Result implications	Effect on innovation
Lack of cooperation between health institutions	Different health institution sits on its proprietary solutions. Implicates sharing of health data and terminate an effective data pipeline	Innovative solutions must be modified to several various health institutions because of the lack of a unified standard.
Need for a national health cloud solution	gives health institution little to no leverage towards suppliers when it comes to expected standards	Innovations are difficult to test as there are no established secure cloud solutions that could feed the innovative system with data.
The “big small data problem.”	While suppliers have use-cases ready for systems that utilise ML, they cannot use it since the data supplied are not structured	1. Discourages startups that utilise emerging technology in other industries to adapt their innovation for the health sector. 2. Unstructured data cant be combined with different types of data to create new health beneficiary innovations.
Data sharing across health institution difficult	Actors with patient journal systems experience a dilemma regarding their privacy and information security when they give document access to other health institutions (I.e. GP’s)	Development for specific segments, and it will only further strengthen the silo-based structure of the healthcare sector.
Standardised code in HIS development	To achieve a greater extent of standardised data in the health sector, the HIS that stores data must be based on standardised code. Elimination of free-text field also contribute to data minimization	With guidelines on standardised code, the development time can be significantly shortened and more easily adapted to different health institutions.

6.4 Tools for regulation and compliance

Risk and vulnerability analysis (ROS - *Risiko- Og Sårbarhetsanalyse*) -, in combination with a Data Protection Impact Assessment (DPIA), help to establish measures to minimize the risk of a security breach happening and to handle potential consequences of such a breach. In the interview with interviewee 6, it was apparent that ROS is a helpful tool for information security assessment. However, there are still difficulties towards entering the health domain with innovations, even though ROS analyses are conducted continuously. Interviewee 6 calls for more precise guidance and guidelines from the public, regarding how architecture and data transfer should be handled.

> *«I think it's a shame that we are all sitting with the same problems separately. Everyone that is innovating new solutions is doing the same type of ROS-analysis and struggling with it. The public sector should have to a greater extent "walked up the trail" for us and made some blueprints for us to base the innovations on».* (Interviewee 6).

Interviewee 6 tells us that it is easy for hospitals to point to GDPR and Normen, but as a supplier, it is difficult to understand what is okay and not okay. To further strengthen this argument, Interviewee 6 followed up with this comment:

> *«Being a supplier, we have experienced that getting our solutions implemented at hospitals are particularly difficult. It's difficult to know what is okay and not okay regarding information security. I feel innovators and entrepreneurs should be offered more knowledge on how to succeed in the public sector».* (Interviewee 6).

Interviewee 7 explains how his company approach ROS-analysis and what it involves; management of everything that falls in the category of personal sensitive data, e.g. name, date-of-birth, illness overview. For every element that will be processed, it has to go through solution design, a description of how the solution technically is set up.
«The ROS-analysis has been challenging because it's a technical ROS-analysis based on implementation test and security. »(Interviewee 7, personal communication).
Furthermore, there is a juridical ROS-analysis conducted based on privacy concerns. The juridical ROS-analysis, in general, suffers from a combination of uncertainty and lack of knowledge. The interpretation of privacy is today very bureaucratic, and in general, there is a lack of a unified interpretation.

DPIA or Data Protection Impact Assessment was another tool that became one of the focus points in our interviews. Opinions and experiences ranged across the whole spectrum, and reveal some very interesting findings. Presented first will be the findings that are related to positive feedback regarding DPIA.

In two of the interviews, it is expressed that the last six months have seen a significant increase in the management focus on DPIA and education and courses around the tool. Both interviewees express that the knowledge growth has been fruitful for their organisations, through the courses' material that shows which consequences and fines municipalities and organisations get when non-compliant.

> *«We have a lot more focus on DPIA these days. DPIA is now a part of the education programme. In fact, we see that the emphasis on DPIA education and the work with DPIA has raised general awareness on the GDPR as well».* (Interviewee 8).

When talking about waterfall versus agile methods within HIS innovation, Interviewee 4 mentions that DPIA is the perfect tool for agile development within the health domain. *«For a big agile development project like this (talking about a national HIS development project), I see DPIA as a perfect tool to uncover measures and gives us the possibility to make necessary adjustments underway».* (Interviewee 8).

Regarding how DPIA could be a barrier for projects or HIS innovation, both interviewee 4 and 7 pointed to time or monetary resources. Interviewee 4 stated that if a project needs an in-advance review from Datatilsynet, it will result in a slowed-down process. Interviewee 7 was very firm when stating that DPIA could have a big impact on the development timeline if not using a pragmatic approach towards DPIA:

> *«DPIA can have a very big impact on the development timeline. It can almost stop and halt everything. This is where it's important to have a pragmatic approach to DPIA because without you could easily sit endlessly and find all types of privacy consequences. Your fantasy is the only limitation».* (Interviewee 7).

Lastly, Interviewee 9 touched upon challenging factors related to the risk-reducing measures that DPIA holds. The measures are many, and according to interviewee 9, it is uncertain to what extent these measures are conducted.

> *«This is a common challenge. So, it's kind of easy to sit down and decide to have that kind of procedure and routine, and we are going to do this and that. If it is actually followed up on is highly uncertain. This is a challenge we have to work through».* (Interviewee 9).

See Table 6.6 for an overview of the theme results.

Table 6.6. Results for the theme of tools for regulation and compliance.

Finding from analysis	Result implications	Effect on innovation
Lack of guidance/guidelines from public	ROS-analysis insufficient to assess architecture and data transfer in the public health sector.	Prolong the process of ROS-analysis novel innovation. Inventors and entrepreneurs could choose to not focus on the health domain if the guidelines are diffuse or unclear. Difficult for innovators to grasp what is okay and not in a hospital setting.
Technical ROS-analysis is challenging	Everything that involves the management of sensitive personal data must go through a solution design to create a description of how every aspect of the solution is set up technically	Put a strain on innovation resources as the process might be lengthy and costly.

Juridical ROS-analysis suffers from uncertainty and lack of knowledge	Interpretation of privacy is very bureaucratic and not unified across the health sector.	Complicates the process of undergoing the juridical part of ROS-analysis.
Work and education on DPIA raise the general awareness connected to GDPR	Knowledge of the regulation is something that is acquired over time.	Strengthens awareness/knowledge on the GDPR for people involved in innovation projects
DPIA perfect tool for agile projects	DPIA is a continuous process. Therefore, it will uncover aspects that need to change in a project	More often than not, innovation project follows an agile methodology. Matching agile development sprints, DPIA is something that is done continuously and is a perfect tool to uncover weaknesses and identify necessary adjustments
Importance of a pragmatic approach to DPIA	Having a pragmatic approach ensures that DPIA does not have a significant impact on the development timeline. DPIA have loose boundaries and can become very time consuming for a project.	For innovations, a pragmatic approach is vital not to slow down the development process. Time = money in projects and monetary resources can often be limited in innovation projects.

6.5 Trust between stakeholders

An emerging pattern within the collected data is the importance of trust between stakeholders when implementing HIS innovations with respect to GDPR compliance. Overall, the companies included in this study see GDPR as a self-certification process, making a claim to be GDPR compliant: *«It's a self-certification process that you only do once. As long as you have an SMS, a Security Management System in place, and the documentation is covered, then you can just claim that you are GDPR compliant.»* (Interviewee 7). Even though organisations can self-certificate on GDPR, the experience is that it's not enough to claim GDPR compliance, building trust and relationships between stakeholders is just as important. In the health sector, a HIS supplier is dependent upon the trust built with the health institutions and community. If something goes wrong in the value chain and data is lost or leaked, even though it is not a suppliers fault, it is still the supplier that gets the hardest critique, and the supplier that sits with the perceived responsibility according to interviewee 7. On the other hand, the public health institutions do not blindly trust a supplier that claims to be GDPR compliant. Throughout the process, since GDPR was implemented through Personopplysningsloven, interviewee 8 experiences that they often uncover major shortcomings in the delivered systems when looking into details while conducting DPIAs. Often the suppliers are not in line with the regulation, and demonstrate a lack of knowledge of the regulation:

> *«Claiming GDPR compliance is not enough. You can't just trust the suppliers, the suppliers are there to sell, and they know we have a strict focus on GDPR… I believe*

> *it's an issue of lacking knowledge of the GDPR at the supplier side when it comes to this. I don't think it's intentional to provide non-compliant solutions, though. »* (Interviewee 8).

Building that trust takes time, and it is essential to be thorough from the start of an innovation process when it comes to innovating regulation-compliant HIS. It can thus be difficult for start-ups and smaller entrepreneurs to sell and implement HIS innovations, as the trust is lacking between them and receiving actor and requires time to build up. A proposed solution for all parties is to think privacy by design from the start. Privacy by design is a requirement that is important to be covered, and interviewee 9 and 4 both hold privacy by design as a checkpoint to cover in the procurement process of HIS innovations. Privacy by design should be done in the early phases of an innovation project (the earlier, the better), and continuously followed throughout the entire process according to interviewee 4, 6, 7 and 8. However, there are some interpretation differences in what privacy by design actually is. Most of the interviewees see privacy by design as a technical aspect that the design itself has codes and features that upholds the concept. Interviewee 4, however, sees privacy by design as not just a method, but a cultural aspect that should be incorporated into the organisation. If you manage to think privacy by design in all aspects of the organisation, business processes and innovative solutions, and get all actors and partners on board with the same interpretation and understanding of privacy by design, it can improve the trust between stakeholders that privacy protection is in fact incorporated into the innovative solutions. Not having an aligned interpretation of privacy by design can act as a barrier to good cooperation between stakeholders.

GDPR compliance is not the only factor that needs to be covered for public health institutions to adopt HIS innovations. Showing professionalism and competence when it comes to change management, developing processes, operations, and exception handling, are just as important. There is also a need to have trust from the consumers when introducing innovative HIS solutions in the healthcare sector. All of the interviewees experience that there is a high trust shown with the healthcare sector from the population and end-users when it comes to protecting the privacy rights of end-users and patients within HIS systems. The end-users of the systems and the population, in general, are perceived to have a higher awareness of data privacy risks and the rights of the individual when it comes to having control over one's own data. It is therefore essential to strive for regulation-compliant HIS innovation to maintain the high trust given to the healthcare sector, and thus be able to implement more innovations to raise the effectiveness and quality of healthcare and health services.

See Table 6.7 for an overview of the theme results.

Table 6.7. Trust between stakeholders

Finding from analysis	Result implications	Effect on innovation
Claiming GDPR compliance not enough	Innovation HIS solutions are often found deficient when it comes to GDPR requirements, even though deemed compliant by the supplier	HIS innovation ideas and solutions are rejected due to different levels of interpretation of what is accepted as compliant solutions between supplier and receiver of HIS innovation.
Trust between stakeholders is important	Building up trust and striving for regulation compliance throughout the innovation process is important for being accepted as a trusted innovator and get innovations implemented.	Documenting GDPR compliance in combination with a high trust between stakeholders generally results in accepted innovation solutions. Gaining that trust is harder for smaller entrepreneurs and startups, thus negatively impacting the acceptance of their innovative solutions in the public healthcare market.
The public generally has high trust in the healthcare sector	Losing the trust of end-users and the population regarding the ability to protect private health data is damaging towards introducing new innovative HIS solutions	HIS innovations are accepted, implemented and used by end-users when there is a high trust in the provider of HIS.
Privacy by design as a culture and method	Incorporating privacy by design as a concept into the culture of the organisation and the relationship between stakeholders raises trust in that innovative solutions are privacy protection centred. Aligning stakeholders in the same interpretation of what privacy by design means eases the cooperation and raises trust between stakeholders.	A unified interpretation and embodiment of privacy by design, and high trust results in better cooperation between stakeholders and regulation compliant innovation.

6.6 Greenfield & Brownfield HIS innovation

The introduction of GDPR has influenced greenfield and brownfield innovation. Brownfield systems are legacy-constrained systems, that is newer systems built upon the old. Greenfield is unconstrained systems, not built on or dependent on old systems (Bohem, 2009). HIS solutions that are made from scratch and are independent of or integrated with pre-GDPR systems can implement the GDPR requirements from the start and become GDPR compliant faster. New systems or modules built upon old, existing systems and infrastructure can often become non-compliant. This is because older systems have not been developed with GDPR in mind. Integrating initially compliant systems and modules into non-compliant existing HIS, causes the new system as a whole to be non-compliant, as evidenced by interviewees 1, 3, 5, 8, and 9. The issue is often that new modules and systems have had limited scope for the DPIAs and risk analysis, focusing on just the new software, not taking the fully integrated system as a whole into account. The effect of this is more time and resources used on fixing holes in the older systems, that could have been fixed or been accounted for in earlier phases of the innovation process: *«There are privacy risk elements that occur when integrating new systems. The risks are not safeguarded by the risk assessments that are done on the new system, because the risk assessments are so narrowly defined.»* (Interviewee 9). The effect has also impacted innovation projects that were under development during the introduction of GDPR. Therefore, finding and fixing non-compliant holes in older systems and reviewing ongoing projects during the implementation of GDPR is slowing down innovation projects. Integrating new systems into old ones reveals bottlenecks when it comes to data privacy security and meeting the GDPR principles. Interviewee 5 has experienced this in the case of giving data back to the individual, the principle of data portability, and so the systems often end up siloed. It is experienced as a general barrier for HIS innovation throughout the Norwegian health sector.

Existing HISs in the public healthcare sector according to interviewee 5 are not approaching GDPR in the same way as newer innovative solutions; for instance, the existing EHR systems. They are seen to be hiding behind the old processes the public healthcare sector has been using and continue as earlier without much innovative progression. The sector points to the Norwegian patient journal law (Pasientjournalloven) and claims that the same integration of GDPR as for new HIS solutions is not possible to achieve within the EHR systems. Several internal, smaller innovative HIS applications were stopped due to the implementation of GDPR, as they were not compliant, mainly due to GDPR requirements of data portability, data minimization and purpose limitation. Such applications were, for instance, locally-made self-registration forms for patients. The applications are abandoned, and it is unclear how the introduction of new technology or smaller updates can be made towards these applications to make them compliant according to interviewee 1. Consequently, an effect of GDPR is that several innovative ideas, pilots and minor HIS applications never reach full implementation.

See Table 6.8 for an overview of the theme results.

Table 6.8. GDPR with Greenfield & Brownfield innovation

Finding from analysis	Result implications	Effect on innovation
Greenfield innovations tend to be GDPR compliant	Innovative HIS solutions built from scratch can comply with GDPR from the start.	Not being dependent on integration with pre-GDPR systems result in GDPR compliant innovations
Integration issues with legacy systems	Fully compliant new innovations become non-compliant when integrated with older systems. Evaluations of the systems as a whole are often not conducted in the early innovation phase of new systems and modules, resulting in compliance issues detected during and after integration.	Pre-GDPR systems act as barriers for innovative progression for HIS.
Existing EHR systems a barrier for HIS innovation	EHR systems built pre-GDPR are utilizing old processes and depends on Norwegian patient journal law. The systems are non-compliant with the GDPR, and innovative solutions integrated with the EHR systems do not become GDPR compliant fully.	Innovations depend on integration with pre-GDPR EHR systems

6.7 GDPR's effect on HIS innovation

Our analysis shows that the GDPR has had effects on HIS innovation. While the concept of protecting sensitive information is seen as a positive and good contribution to protecting the data of the individual, there is an uncertainty towards what the GDPR actually means, and how it's supposed to be applied in HIS initiatives. *Figure 6.2* shows on a high-end level how the GDPR is affecting HIS innovation in the Norwegian healthcare sector.

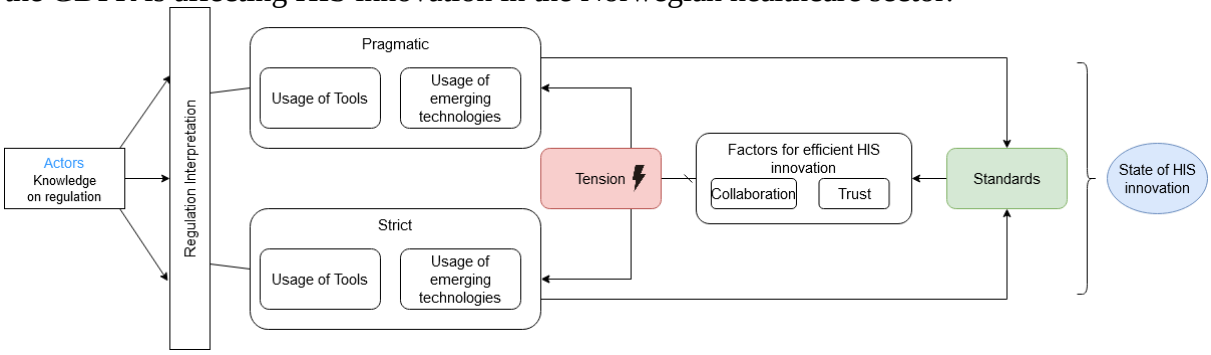


Figure 6.2. A holistic view of GDPR's effect on HIS innovation in the Norwegian healthcare sector

There are different interpretations of the regulation, and some organisations have stricter enforcement of the regulation than others. Furthermore, the public healthcare sector uses Normen, which gathers data security, privacy regulation and other relevant health legislature and sums it up with a corresponding checklist-tool to aid in innovating compliant HIS as well as other data gathering and processing solutions. However, the same issues of lack of education and training, as well as interpretation, are apparent in the analysis results regarding the use of Normen for privacy compliance. Strict enforcement of privacy regulation is especially apparent in public hospitals, where the interpretation of the regulation is strict. Private entrepreneurs experience difficulties when trying to work with hospitals and develop HIS, and there is not enough clarity in guidelines and standards to aid the entrepreneurs in developing HIS that is deemed compliant according to hospital requirements. This drives up the resource cost and time used to develop the HIS innovations, and often results in slowed down or abandoned projects. This is especially seen with cloud computing solutions, as hospitals as data controllers are reluctant to use public cloud providers or HIS that is built on public cloud infrastructure. Municipalities, however, actively use cloud solutions in primary care, and the findings illustrate that there are different approaches and levels of regulation interpretation and enforcement between primary and special healthcare providers.

The use of ML algorithms and AI is at the pilot and testing stage, and not implemented for medical analysis purposes in a production setting in the Norwegian healthcare sector. Issues regarding consent to use sensitive data is halting the introduction of ML and AI innovative solutions, because gathering consent to analyse millions of journal documents and data is practically difficult due to the vast number of affected individuals. The principle of data minimization plays a significant role here as well. Furthermore, sharing data between HIS systems is difficult as sector-wide standards for the structuring of data is not implemented. There is thus a challenge when trying to share large amounts of unstructured data between systems, and to usefully process the unstructured data.

The use of tools for regulation compliance also impacts the innovation process. Using DPIAs and continuously updating and reviewing them, especially in an agile development setting, aids in developing a regulation-compliant end-result. However, the findings show that risk analysis and DPIAs are conducted without a specific sector-wide standard or guideline. Organisations with a strict interpretation of the regulation will experience discovering issues without end. A suggested solution in the findings for this issue, is to have a more pragmatic approach to DPIA and risks, loosening up the strict interpretation of the regulation. Apparent in the findings is that establishing standards for regulation compliance for HIS innovation and a unified interpretation of the regulation would benefit innovation processes and outcomes and make it easier to establish cooperation between stakeholders.

Claiming GDPR compliance is not enough; trust must be established between stakeholders to attain productive innovation processes and faster adoption of innovative solutions. A unified interpretation of the privacy by design principle, standards and guidelines for regulation compliance, can positively raise trust between stakeholders, improve cooperation, and result in more adopted HIS innovation.

7. Discussion

This chapter discusses the findings of the data analysis in relation to related literature and presented theoretical concepts. The chapter also discusses the study limitations.

According to Blind et al. (2017), regulations will affect innovation differently, depending on the uncertainty that lies in the market. Regulation will have a different effect on innovation efficiency depending on the level of market uncertainty. Specifically, in the case of high market uncertainty, regulations impose a higher degree of compliance and innovation costs due to information asymmetry. This information asymmetry derives from the top-down approach and the differences in knowledge on specific technology between the governing actor and the market actors. The mismatch and gap in knowledge are further increased in markets characterised by rapidly changing heterogeneous technical landscapes (Blind et al., 2017). We argue that the Norwegian health sector is an uncertain market to innovate in. The grounds for this claim within our findings are linked to the statements about the technological complexity of the architecture Norwegian healthcare builds upon. This technological complexity is observed for instance in the finding that it is hard to share health data between health institutions. Actors who want to share data from their patient journal systems with other actors that are not using a patient journal system, encounter this complexity. Another aspect that strengthens our claim that the Norwegian health sector is an uncertain market, stems from the revelation that there is a severe lack of cooperation between health institutions. Our findings reveal how different health institutions having their own proprietary solutions complicates the sharing of health data and terminates an active data pipeline. This finding shows how technological solutions are competing with each other and that there is a presence of technological heterogeneity.

7.1 Different interpretations of GDPR and regulation knowledge gap

Our study shows that after almost two years since the complete implementation of GDPR into Norwegian privacy legislation, there is inadequate knowledge on the regulation.
Several of our findings are in line with Blind et al. (2017) and show how privacy regulation has a negative impact on innovation efficiency in the Norwegian health sector. But instead of revealing a potential lack of knowledge on specific technology from legislators, we discovered that the lack of knowledge lies with market actors and across many organisational levels of the health sector with respect to the interpretation of the GDPR. GDPR is interpreted differently across the health sector. GDPR is experienced to be a gigantic regulation affecting technology, work processes, and the culture both within organisations and the health sector. The various interpretations and lack of knowledge on the regulation is affecting both internal cooperation between leaders and employees in organisations and cooperation between stakeholders. This has affected innovation processes negatively, as innovators must change their focus to understanding and grasping privacy regulation rather than focusing on the innovation itself, which in turn, raises the monetary cost of innovation projects and much time is spent on discussions and developing a common understanding of the regulation and measures that must be taken to be compliant.

The findings further show that issues of uncertainty and lack of knowledge on the GDPR, along with what the GDPR requirements are in the case of HIS innovation, are further magnified when considered in relation to lawyers and data protection officers. Developers are turning to leaders to be guided on the requirements of privacy regulation, and leaders turn to lawyers and data protection officers. When there is uncertainty of how the regulation is to be

interpreted, confusion arises, resulting in delayed or halted HIS innovation projects. Having a good collaboration between health professionals, SMEs, developers, and policymakers is vital for the success of implementing HIS innovation initiatives (Swinkels et al., 2018), and the knowledge gap and uncertainty regarding GDPR is negatively affecting cooperation on HIS innovation initiatives in the health sector. We argue that there is a need for a clear and unified interpretation of the regulation to which actors in the health sector can align towards, and a high focus on training and educating on privacy regulation can help fill the knowledge gap in the sector.

7.2 GDPR and emerging technologies in the health sector

According to Martin et al. (2019, p. 1311), strict regulatory enforcement and demand for compliant products give little incentive for innovation with non-compliant products, and there is to be expected high regulation compliance, regulation exploiting innovations, and a high level of innovation abandonments. This relates to our findings that public hospitals are considered to be very strict in their interpretation of privacy regulation. This strict interpretation has resulted in accepted HIS innovations into hospital settings that are highly compliant with the regulation, but also results in many innovation possibilities not being explored or adopted, like AI, ML and public cloud solutions.

While there was a broad consensus from the findings that AI would benefit efficiency and deliverance of healthcare services, it was acknowledged that the strict regulatory enforcement creates hurdles for practical use of AI. With purpose limitation as one of the core principles of GDPR (Regulation (EU) 2016/679, 2016, p. 35-36), a hurdle is created for gathering enough data for AI to have reasonable benefits. The challenge identified is in line with the findings of Martin et al. (2019 p. 1319), that innovations which are data-driven are severely limited by, (1) data-processing having a legal basis, and (2) purpose limitations. Stakeholders are positive and see the potential benefit of AI. Still, due to the strict regulatory enforcement that is apparent in the Norwegian health sector, as well as the regulation principles of consent, legal basis, and data minimization, AI innovation projects are “stuck” in a pilot or testing environment and never see full implementation. A potential outcome scenario might be that suppliers or innovators that create software based on emerging technologies are deterred from adapting their software to healthcare, resulting in product abandonment as outlined by Martin et al. (2019 p. 1319). We also identify how the uncertainty about how AI processes data and draws its conclusions (Datatilsynet, 2018, p. 18), does not fit with GDPR’s principle of transparency and accountability. In addition, statements regarding the problematic area of consent for data used by AI surfaced in interviews. Since all data belong to an individual and individuals have unique rights concerning GDPR, data processors must ask for consent in advance if they are to use patient data for research purposes. This is very troublesome if the data for research are based on millions of patient journal entries. This adds another layer of obstructions for the potential use of innovative solutions that build upon AI as a technology, since article 22 of GDPR (Regulation (EU) 2016/679, 2016, p. 46) states that data subjects have the right not to be subject to a decision based solely on automated processing, which produces legal effects concerning him or her. This is in line with the statement from Martin et al. (2019 p. 1317-1321) on how innovations dealing with large amounts of data can be troublesome in the context of consent to use personal information. This conflict between privacy and potential health benefitting services of AI, can establish a dilemma that currently has significant implications for innovative AI solutions that otherwise could potentially be utilised in the Norwegian public health sector. While the analysis of the collected data in this study shows that AI, today, is not widely used in the Norwegian health sector, ML algorithms and AI software and solutions are seen as a positive contributor to

raise healthcare quality. Stakeholders within the health sector are positive towards exploring future possibilities connected to AI as a means to improve healthcare services. This can foster new regulation exploiting innovations that contribute to the tenet of making AI solutions that are regulation compliant.

Solving the puzzle of privacy versus the usage of AI/ML may create a ripple effect that has positive consequences for HIS innovation as a whole. There are several HIS innovations that are dependent on AI/ML as a technology. Health information systems such as the ML information extraction system described by Hassanpour & Langlotz, (2016), or the usage of ML for creating prediction models for colorectal cancer by extracting data from EMR (Hoogendoorn, Szolovits, moon & Numans, 2016, p.16.) can potentially be realised. Big data gives the health domain a unique opportunity to analyse everything from basic structured patient information to unstructured image data from EHR databases. The technology is available, and it allows a more detailed investigation of diseases that can be faster, broader, and more unbiased (Gu et al., 2017, p. 30-32).

The same potential outcome is also relevant for innovations that utilise cloud computing. Findings indicated that due to the strict interpretation of privacy regulations, public hospitals do not accept and implement external cloud-based HIS innovations. It is important to recognise that, in contrast to public hospitals, several municipalities and primary healthcare in local communities take advantage of cloud-based HIS. This difference in choice means there are different interpretations of GDPR in different levels of public healthcare.

A finding identified in interviews that were connected to GDPR and cloud computing was the call for a national health cloud solution. Interviewees from both suppliers and healthcare expressed that a cloud solution that spans across all health institutions and gives access to real test data, is severely needed for the Norwegian health sector to advance in line with technological advancement. As noted by Gu et al. (2017, p. 30-32), cloud computing could have the potential to solve some of the storage and data-sharing issues that were identified through the interviews. If the strict interpretation of the usage of cloud computing to store and process data is not changed, this will have a negative impact on HIS innovation since there will be difficulties in establishing secure cloud solutions to feed innovative systems with necessary test data.

7.3 Integrating new innovative solutions with legacy systems

Our findings indicate that greenfield HIS innovation can be made compliant from the start of the innovation process. This is because the innovations can implement privacy by design and privacy by default principles early in the process. In an environment with strict regulatory enforcement of GDPR, greenfield innovations can be designed with a strict emphasis on compliance, without changing the systems infrastructure it is built on. In such a strict environment, there will be a high level of innovative, compliant solutions (Martin et al., 2019, p. 1311-1312). This is also evident in the health sector. The strict interpretation and enforcement, encourages innovative solutions to be compliant with the GDPR and we argue that this is also the case for HIS innovation, in line with Martin et al. (2019). The findings reveal that the GDPR has had an innovation constraining effect on brownfield HIS innovation initiatives. For HIS brownfield innovations, the legacy systems must be re-designed with privacy-enhancing and security-enhancing technologies and software (Tamburri, 2020, p.12).

We argue, based on our findings, that the re-design of legacy systems to comply with GDPR is a resource and time-demanding task, raising the overall cost of innovation projects. High costs which potentially breach budgets and not meeting time goals, increasingly raises the risk of an innovative project failing (Schwalbe, 2019, p. 15-16; Hughes et al., 2016). The findings reveal that older HIS systems are not designed with GDPR in mind; although earlier privacy laws were strict, the GDPR raised the awareness of the need for privacy protection solutions. This has resulted in new system enhancements and modules, and smaller systems integrated into older systems might be compliant with the regulation as compliance has been highly focused. However, not re-designing the legacy systems, results in the new systems as a whole being non-compliant. Our findings show that not re-designing legacy systems and fixing security and privacy issues in the old systems is occurring with brownfield HIS innovation initiatives. A reason for this is often that the innovators focus the DPIAs and risk assessments on the new modules, systems or enhancements, not evaluating the entire system, including legacy systems as a whole. This can result in new solutions being abandoned or rejected, and more time and resources must be used to enhance regulatory compliance. The findings also show that it is difficult to implement solutions for data portability in old HIS, and this is experienced as a barrier for innovation in the health sector. When organisations also have different interpretations and stick to old processes, claiming that GDPR compliance cannot be fully integrated into existing EHR systems, this acts as a barrier for new HIS innovative solutions to utilise the old EHR systems. We thence argue that the GDPR has had a short-term negative effect on brownfield HIS innovation, raising the innovation costs and slowing down innovation progress. We find no empirical evidence on how the GDPR affects brownfield HIS innovation in the long-term. An argument could be made that, as more legacy systems are re-designed, the introduction of new compliant solutions will be easier, as the total systems will be more compliant. However, this is a prediction without a basis in the findings of this study or literature.

7.4 Standards in the Norwegian health sector

The results of this study indicate that there is a need, expressed in the health sector, for industry standards regarding privacy and security. Notably, the need for national standards with regards to data sharing and cloud solutions. The GDPR is experienced as very abstract and weakly technology-specific when it comes to cloud computing solutions, and the difference in regulation interpretation between actors creates difficulties for collaboration and data sharing. This experience of the GDPR as a top-down regulation, with the misfit between regulation and technology, is in accord with Blind et al. (2017) model. As the Norwegian health sector is an uncertain market, the GDPR does not account in detail for specific technology paths. According to Blind et al. (2017), innovation efficiency is negatively impacted by regulation in this type of market, and industry standards derived from a process-driven market approach would benefit innovation positively. The findings reveal a need for an industry standard for cloud solutions and data sharing on a national level. Also, the need for standardised code for HIS development would benefit HIS innovation, as standardised code deemed compliant with the GDPR would make the process of innovating HIS solutions easier since the code structure can be applied and reviewed for compliance in an agreed manner.

There is, however, an attempt to sum up and simplify the complex interaction between multiple crossing legislations for data security and privacy in the health sector. Normen, as a tool and framework, is developed by market actors in the health sector and covers important legislations and requirements that must be covered in a HIS solution for innovations to be

compliant and accepted in the public health sector (Direktoratet for e-Helse, 2020a). Our findings show that Normen is accepted as a tool and frequently used in the health sector for HIS innovations. Normen is, however, experienced by some actors in the market to be comprehensive and non-differentiable to the size of the organisations. Although there is a version targeting small enterprises and individuals (Direktoratet for e-Helse, 2019b), the findings reveal that there is still a need for sound training in the framework and knowledge of GDPR and other relevant legislation to be able to use Normen as intended. Normen is experienced as a tool for management, and developers have a hard time grasping which parts of Normen are relevant for them and how to use Normen. We argue that raising knowledge on privacy with education on Normen, could lower the interpretation difference of privacy regulation in the market. Smaller actors and start-ups should review Normen and consider using it and strive to comply with the requirements to innovate solutions that are accepted in the public sector. The continuous work on improving Normen as tool and framework would benefit the market by targeting specific technology paths, like cloud computing, to create guidelines and standards that can unify the market with fewer interpretation gaps- and less uncertainty on how to comply with the GDPR.

7.5 Trust, tools and collaboration

The results of this study lead to the realisation that different actors in the Norwegian health sector utilise tools for regulation and compliance differently. While ROS is described as a helpful tool for suppliers, with respect to information security, suppliers still describe a discrepancy in what hospitals ask for and what is assessed in a ROS-analysis. This complicates the processes of introducing innovations to the Norwegian health domain market. According to our findings, there is a lack of more precise guidelines from the public sector regarding information security in architecture and data transfer. ROS-analysis is required by law, but our findings show that standards, or a closer collaboration between public and private organisations, need to be strengthened. This relates to what Bazzoli et al. (1997) state about the importance of cooperation between public and private actors to overcome the apparent growing constraints related to resources and time. This challenge has direct consequences on innovation, since the lack of guidelines from the public sector may severely prolong the process of ROS-analysis for novel health innovations. If the guidelines are diffuse and difficult to interpret, the innovator may be discouraged from pursuing the health domain as a market for their innovation. This need for standards to enable collaboration and trust, can also be seen in our visualised overview of GDPR's effect on innovation, Figure 6.2.

Our findings showed the same pattern regarding DPIA. The experiences and thoughts on the tool are varied depending on what type of organisation interviewees represented. Since DPIA is something that is done continuously, it was described as the perfect tool for agile projects. We identify this as a positive impact on HIS innovation since, according to the findings, more often than not, innovation projects follow an agile methodology. The results of this study suggest, that if done continuously, DPIA can match agile development sprints and consecutively uncover weaknesses and identify necessary adjustments. Also, our findings revealed that mandatory work on DPIA raised general awareness regarding GDPR for workers involved in an innovation project.

One interviewee pointed to how a pragmatic approach to DPIA is vital to ensure that the innovation development timeline will not be affected negatively. Since DPIA has relatively loose boundaries, it can become very time consuming for an innovation project. A lack of a

pragmatic approach will directly affect innovation by putting additional resource constraints on innovation projects.

7.6 Summary

The GDPR has had both negative and positive impacts on HIS innovation in the Norwegian health sector. Several themes have surfaced through the analysis of interviews conducted with different healthcare actors. Firstly, the various interpretations of GDPR and a general regulation knowledge gap have affected innovation. New roles are established, and employees with specialization need to expand their knowledge and change the focus away from their innovation. Uncertainty of how one should interpret the regulation have implications for collaboration between healthcare actors, and further increase the issues of introducing innovation in the health sector. We argue for a more precise and unified interpretation of the regulation that all health sector actors can align towards.
The innovations accepted in hospitals are highly compliant with the regulation, but according to the findings, many innovation possibilities are not being explored or adopted. The regulation severely limits innovation connected to AI or ML as principles such as consent, legal basis, and purpose limitation, are difficult to handle in such technologies. The potential outcome is that suppliers and innovators who create software based on emerging technologies are deterred from adapting their solutions to the health sector.

Our findings revealed a need for an industry standard for cloud solutions and data sharing on a national level. Furthermore, the use of standardised code would contribute to HIS innovation becoming GDPR compliant. Normen, is the market actors' attempt to create a cross-organisational standard. It simplifies the complex interaction between multiple legislations for data security and privacy. Issues regarding knowledge connected to usage of Normen, and the lack of differentiation for the size of organisations were identified through the research. We argue that knowledge raising on Normen, across all the industry levels would reduce the difference in interpretation of privacy regulation in the market.
The findings revealed a lack of precise guidelines from the public sector regarding information security in architecture and data transfer. The use of tools such as ROS-analysis and DPIA is directly affected by the lack of precise guidelines, as there is a discrepancy in the interpretation of the regulation demands. Furthermore, there is a need for strengthening the collaboration between private organisations to establish standards and trust, as well as the apparent growing constraints related to resources and time.

7.7 Limitations

Naturally, our study has limitations. Firstly, the choice of theoretical lenses and method might limit the results of this study, as other theories or concepts and methods might give additional insight into the phenomena. However, the choice of theoretical lens and research design is conducive to exploring and interpreting the phenomena acknowledging that there is not a single answer to our problem statement. The timing of this study is also an important factor affecting our results. As the GDPR is relatively new, long-term effects of the regulation on HIS innovation might not be revealed in our results. Nevertheless, the findings on short-term effects give valuable insights and can be a basis for continuous study and future research on the effects of privacy regulations on HIS innovation.

The study is limited to Norwegian healthcare actors on purpose, but also for logistical reasons. As the transcription of GDPR in national laws and regulations is country-specific, confining the research to within Norway ensured that regulatory variations do not blur the results. Furthermore, it was desirable to delimit the research to local actors so that interviews could be conducted in person.

Our study was limited to interviewing top and mid-level information security and privacy officers and leaders. A consequence of this is that the study does not include the experiences and interpretations of operational level employees. Researching the perspectives of operational level employees is an interesting avenue for further research.

8. Conclusion and implications

The main aim of this study was to investigate the effects the GDPR has on HIS innovation, and the responses that the health sector and IS providers apply to innovate regulation-compliant solutions and meet constraints set by GDPR. In this study, our research questions were:

(1) *How does the General Data Protection Regulation affect health information system innovation for personal health information sharing initiatives?*

(2) *What concrete responses do companies apply to health information system initiatives to meet constraints set by the General Data Protection Regulation?*

The results of this study indicate that the implementation of GDPR has had both innovation driving and hindering effects on HIS. There is a knowledge gap amongst management, HIS innovation project members and developers regarding the GDPR. As actors are uncertain of how to interpret the GDPR, there are various approaches to this in the Norwegian healthcare sector, where public hospitals are, in particular, seen to have a very strict approach to the interpretation and enforcement of privacy law. This strict interpretation and enforcement of privacy regulations act as a barrier for entrepreneurs and HIS start-ups to enter the market with innovative HIS. Tension between actors with strict interpretation and actors with a pragmatic interpretation of the regulation can thus occur. The healthcare sector has developed an industry norm, Normen, which summarises essential data security and privacy legislation for the healthcare sector and is applied to achieve regulatory compliance. It can be used as a tool, together with DPIA, and risk and vulnerability assessments, to ensure compliance and HIS solution acceptance. However, the results reveal that Normen, like the GDPR, is experienced as complicated and challenging to apply, and it can be resource-draining to learn and use. Often smaller enterprises and HIS providers struggle to pinpoint which requirements of Normen apply to the innovative solutions they develop.

The principles of the GDPR, in combination with the variability in interpretations and uncertainty towards the regulation, has affected HIS innovation building on public cloud solutions, AI and ML. Compliant HIS innovation occurs with greenfield innovation, as implementing privacy requirements on new systems is easier when done from scratch. However, the process of doing brownfield innovation has been draining resources and time as old systems are non-compliant with the regulation and are often not accounted for in risk and vulnerability assessments and DPIA until late in the project. The GDPR has thus had positive effects on HIS innovation for regulation-compliant HIS, but also negative effects have occurred because of different interpretations and enforcement levels of the regulation, resulting in delayed or abandoned HIS projects, often with high resource drains.

8.1 Implications for Practice

The strict interpretation and enforcement of privacy regulation, especially amongst Norwegian public hospitals, acts as a barrier for suppliers of HIS innovations. The use of Normen to evaluate regulation compliance of HIS innovations is important to get products accepted and adopted. However, as Normen is experienced to be complicated and complex, further development of Normen is needed to clarify regulatory requirements for smaller entrepreneurs and start-up companies. Additionally, there is a need for training and education on privacy regulations for HIS amongst both management and project teams for organisations that innovate and implement HIS solutions.

Although HIS suppliers can document GDPR compliance, this is not enough, as trust between stakeholders is important for the acceptance and adoption of HIS innovative initiatives. To clarify the requirements that the regulation imposes on HIS innovation in a strict regulatory environment such as the public health sector, standards for data security and privacy can be implemented. The standards might aid in addressing the challenges and information asymmetry that the GDPR has raised, especially towards emerging technologies in the health sector, as also suggested by Blind et al. (2017) for innovation in uncertain markets. We argue that raising general knowledge of the GDPR, aligning regulation interpretation and introducing standards might also aid HIS suppliers to build trust with the public health-sector organisations.

8.2 Implications for Theory

Blind et al. (2017, p. 253) argue that in markets that are characterized by rapidly changing and heterogeneous technical landscape, a technological mismatch appears. This mismatch is generated due to information asymmetry. The less known about the innovation, the more ambiguous the regulation, and hence more uncertainty is felt by innovators. We have shown that this applies to the Norwegian health sector, where findings indicate uncertainty by innovative suppliers, but also the request for more specific guidelines connected to innovation utilising specific emerging technologies. Regarding Martin et al. (2019) statement that regulation is both constraining and stimulating, our findings are concordant. The enforcement of privacy by design, a significant aspect of the GDPR, was seen as a potential driver for cooperation and for enabling regulation-compliant innovation. Constraints were also apparent through the findings. Our research can be seen as a supplement to existing research that brings insights related specifically to the healthcare domain in Norway. These insights are graphically represented in the model of GDPR's effect on HIS innovation in the Norwegian healthcare sector shown in Figure 6.2.

8.3 Concluding remarks

In this thesis, we investigated how GDPR affects HIS innovation in the context of the Norwegian health sector. We use a qualitative research method, and data is acquired by utilising semi-structured interviews. Interview candidates were identified through networks and snowballing. The data is analysed through several iterations using thematic analysis. Empirical evidence that forms the basis of the findings, are presented both through free-text and quotes. In addition, the findings are structured in tables to aid readability.
Findings are then discussed and seen in the context of related research and theory. A lack of knowledge and variation in interpretation of the regulation was identified as one of the main findings. Furthermore, unclear regulation and guidelines related to emerging technologies have created issues for HIS innovation. Lastly, the establishment of more precise standards

by market actors to strengthen collaboration and trust is suggested as a potential solution to some of the issues that are apparent in present HIS innovation.

8.3.1 Recommendation for future research

This thesis analysed collected data with a focus on how the GDPR affect HIS innovation, and what responses health organisations apply to meet constraints set by the GDPR. It would be of interest to investigate the effect of GDPR on HIS innovation in the long term. Furthermore, researching the perspectives of operational level employees is an interesting avenue for further research. Also, further studies are needed on the effect of standardisation on HIS innovation, and if standardisation yields positive effects on HIS innovation with regards to the privacy regulation. Future research should focus on solutions for better privacy regulation-compliant and streamlined data sharing between health initiatives and HIS solutions. This research direction can benefit from an exploration of standards that are present in the Norwegian health industry, and the identification of specific standards that could potentially be implemented to facilitate stronger cross-organisational collaboration and trust between actors.

9. References

Angst, C. M., & Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS quarterly, 33*(2), 339-370.

Appelbaum, S, H. (1997). Socio-technical systems theory: an intervention strategy for organisational development. *Management Decision, 35*(6), 452-463.

Ariens, L. F., Schussler-Raymakers, F. M., Frima, C., Flinterman, A., Hamminga E., Arents, B. W., Bruijnzeel-Koomen, C.A, de Bruin-Weller, M.S. & van Os-Medendorp, H. (2017). Barriers and Facilitators to eHealth Use in Daily Practice: Perspectives of Patients and Professionals in Dermatology. *Journal of Medical Internet Research, 19*(9). DOI: 10.2196/jmir.7512

Bazzoli, G. J., Stein, R., Alexander, J. A., Conrad, D. A., Sofaer, S., & Shortell, S. M. (1997). Public-private collaboration in health and human service delivery: Evidence from community partnerships. *The Milbank Quarterly, 75*(4), 533-561.

Baregheh, A., Rowley, J., & Sambrook, S. (2009). Towards a multidisciplinary definition of innovation. *Management decision*. DOI: 10.1108/00251740910984578

Berner, E. S. (2007). *Clinical decision support systems* (Vol. 233). New York: Springer Science+ Business Media, LLC.

Bessant, J., Lamming, R., Noke, H., & Phillips, W. (2005). Managing innovation beyond the steady state. *Technovation, 25*(12), 1366-1376.

Bidmead, E., Reid, T., Marshall, A., & Southern, V. (2015). "Teleswallowing": A case study of remote swallowing assessment. *Clinical Governance, 20*(3), 155-168.

Blind, K., Petersen, S, S. & Riillo, C, A, F. (2017). The impact of standards and regulation on innovation in uncertain markets. *Research policy, 46* (1), 249-264. DOI: https://doi.org/10.1016/j.respol.2016.11.003

Bohem, B. (2009). Applying the Incremental Commitment Model to Brownfield System Development. *7th Annual Conference on Systems Engineering Research.* Retrieved from https://pdfs.semanticscholar.org/d44a/10e52f025ae5a3228578a7d1d6cf4735b019.pdf

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

Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J. & Neville, A, J. (2014). The Use of Triangulation in Qualitative Research. *Oncology Nursing Forum, 41*(5), 545-547.

Christensen, F. & Næss, P. S. (2019). *Barriers in eHealth initiatives, a literature review.* Unpublished manuscript, Kristiansand: Universitetet i Agder.

Daim, T. U., Behkami, N., Basoglu, N., Kök, O. M., & Hogaboam, L. (2016). Healthcare Technology Innovation Adoption. Innovation, Technology, and Knowledge Management.

Datatilsynet. (2018). *Kunstig intelligens og personvern.* Retrieved from https://www.datatilsynet.no/regelverk-og-verktoy/rapporter-og-utredninger/kunstig-intelligens/

Direktoratet for e-helse. (2017). *Årsrapport for Direktoratet for e-helse 2017.*(Mars 1st 2020). Retrieved from https://ehelse.no/publikasjoner/arsrapport-for-direktoratet-for-e-helse-2017

Direktoratet for e-helse. (2019a). *Rettslige grunnlag for behandling av helse- og personopplysninger i GDPR.* Retrieved 22.04.2020 from https://ehelse.no/personvern-og-informasjonssikkerhet/rettslige-grunnlag-for-behandling-av-helse-og-personopplysninger-i-gdpr

Direktoratet for e-helse. (2019b). *Veileder for små helsevirksomheter* (Version 1.0). Retrieved from https://ehelse.no/normen/veiledere/veileder-for-sma-helsevirksomheter

Direktoratet for e-helse. (2020a). *Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren* (Version 6.0.). Retrieved from https://ehelse.no/normen/normen-for-informasjonssikkerhet-og-personvern-i-helse-og-omsorgssektoren

Direktoratet for e-helse. (2020b). *Normen versjon 6.0*. Retrieved from https://ehelse.no/normen/aktuelt-om-normen/normen-versjon-6.0

Direktoratet for e-helse. (2020c). *Oversikt over Normens krav.* (Version 1.0). Retrieved from https://ehelse.no/normen/normen-for-informasjonssikkerhet-og-personvern-i-helse-og-omsorgssektoren

Efta. (n.d). *European Economic Area (EEA) / Relations with the EU.* Retrieved April 21st 2020 from https://www.efta.int/eea

European Data Protection Supervisor. (2019). *The history of of the General Data Protection Regulation.* Retrieved from URL: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

Flick, U. (2007). *Managing Quality in Qualitative Research.* London: Sage Publications Ltd.

Grisot, M., Hanseth, O. & Thorseng, A. A. (2014). Innovation Of, In, On Infrastructures: Articulating the role of architecture in Information infrastructure evolution. *Journal of the Association for Information Systems, 15*(4). DOI: 10.17705/1jais.00357

Gu, D., Li, J., Li, X. & Liang, C. (2017). Visualizing the knowledge structure and evolution of big data research in healthcare informatics. *International Journal of Medical Informatics, 98,* 22-32. DOI: http://dx.doi.org/10.1016/j.ijmedinf.2016.11.006

Hanseth, O., Bygstad, B., Ellingsen, G., Johannessen, L. K., & Larsen, E. (2012). ICT standardisation strategies and service innovation in healthcare.

Hardless, C. & Jaffar, A. (2011). Heterogeneous Inter-Organisational IT Innovation Creation: Institutional constraints in a public sector oriented market. *Scandinavian Journal of Information Systems, 23*(1), 29-58. https://aisel.aisnet.org/sjis/vol23/iss1/2/

Hassanpour, S. & Langlotz, C, P. (2016). Information extraction from multi-institutional radiology reports. *Artificial Intelligence in Medicine, 66,* 29-39. DOI: http://dx.doi.org/10.1016/j.artmed.2015.09.007

Haux, R. (2006). Health information systems – past, present, future. *International Journal of Medical Informatics, 75,* 268-28. DOI:10.1016/j.ijmedinf.2005.08.002

HealthIT.gov. (2020a). *What is an electronic health record(HER)?.* Retrieved May 21th 2020 from URL: https://www.healthit.gov/faq/what-electronic-health-record-ehr

HealthIT.gov. (2020b). *What is the difference between electronic health medical records, electronic health records and personal health records?*. Retrieved May 21th 2020 from URL: https://www.healthit.gov/faq/what-are-differences-between-electronic-medical-records-electronic-health-records-and-personal

Helsenorge. (n.d). *Private behandlingssteder med avtale.* Retrieved April 20th 2020 from https://helsenorge.no/velg-behandlingssted-seksjon/Sider/private-behandlingssteder.aspx

Hoogendorn, M., Szolovits, P., Moons, L, M, G. & Numans, M, E. (2016). Utilizing uncoded consultation notes from electronic medical records for predictive modeling of colorectal cancer. *Artificial Intelligence in Medicine, 69,* 53-61. DOI: https://doi.org/10.1016/j.artmed.2016.03.003

Hughes, D, L., Rana, N, P., Simintiras, A, C. (2016). The changing landscape of IS project failure: an examination of the key factors. *Journal of Enterprise Information Management, 30*(1), 142-165. DOI: 10.1108/JEIM-01-2016-0029

Jasmontaite, L., Kamara, I., Zanfir-Fortuna, G. & Leucci, S. (2018). Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR. *European Data Protection Law Review, 4*(2), 168-189. DOI: https://doi.org/10.21552/edpl/2018/2/7

Kenny, G., O'Connor, Y., Eze, E. & Heavin, C. (2017). Trends, Findings, and Opportunities: An Archival review of health information systems research in Nigeria. *Journal of the Midwest Association for Information Systems, 2*(6). https://aisel.aisnet.org/jmwais/vol2017/iss2/6

Knight, A. W., Szucs, C., Dhillon, M., Lembke, T., & Mitchell, C. (2014). The eCollaborative: using a quality improvement collaborative to implement the National eHealth Record System in Australian primary care practices. *International journal for quality in healthcare*, *26*(4), 411-417.

Laudon, C, K. & Laudon, J, P. (2016). *Management Information Systems Managing the Digital Firm* (14th ed.). Essex: Pearson Education.

Lessig, L. (2001). "The Law of the Horse: What Cyberlaw Might Teach." Harvard Law Review 113: 501-546.

Leung, L. (2015). Validity, reliability and generalizability in qualitative research. *J Family Med Prim Care*, *4*(3), 324-327. DOI: 10.4103/2249-4863.161306

Martin, M., Matt, C., Niebel, C. & Blind, K. (2019). How Data Protection Regulation Affects Startup Innovation. *Information Systems Frontiers, 21*, 1307-1324. DOI: https://doi.org/10.1007/s10796-019-09974-2

Menon Economics. (2019) Helsenæringens verdi 2019 (Menon publikasjon nr. 24/2019) Retrieved from: https://www.nho.no/siteassets/helsenaringens-verdi-2019.pdf

Misser, N. S., Jaspers, J., van Zaane, B., Gooszen, H. & Versendaal, J. (2018). Transforming operating rooms: factors for successful implementations of new medical equipment. *BLED eConference 2018 Proceedings. 24*, 279-290. DOI https://doi.org/10.18690/978-961-286-170-4.18

Manogaran, G., & Lopez, D. (2017). A survey of big data architectures and machine learning algorithms in healthcare. *International Journal of Biomedical Engineering and Technology*, *25*(2-4), 182-211.

Oates, B, J. (2006). *Researching Information Systems and Computing.* London: Sage Publications Ltd.

OECD. (2017). *OECD Reviews of Innovation Policy, Norway 2017.* Paris: OECD Publishing. DOI: https://doi.org/10.1787/9789264277960-en

Ochieng, P. A. (2009). An analysis of the strengths and limitation of qualitative and quantitative research paradigms. *Problems of Education in the 21st Century*, *13*, 13.

Oh, H., Rizo, C., Enkin, M., & Jadad, A. (2005). What is eHealth?: a systematic review of published definitions. *World Hosp Health Serv*, *41*(1), 32-40.

Personopplysningsloven. (2018). Lov om behandling av personopplysninger (personopplysningsloven) (LOV-2018-06-15-38). Retrieved from https://lovdata.no/dokument/NL/lov/2018-06-15-38

Politidirektoratet, (2017). *Trusler og utfordringer innen IKT-kriminalitet.* Retrieved from URL: https://www.politiet.no/globalassets/dokumenter/pod/ikt_krim_pod.pdf

Pramanik, P. K. D., Pareek, G., & Nayyar, A. (2019). Security and Privacy in Remote Healthcare: Issues, Solutions, and Standards. In *Telemedicine Technologies* (pp. 201-225). Academic Press.

Qsrinternational. (2020). *Unlock insights in your data with powerful analysis.* Retrieved 21.03.2020 from https://www.qsrinternational.com/nvivo-qualitative-data-analysis-software/home

Regjeringen. (2019, 14. January). *Film om korleis Noreg styres.* Retrieved from https://www.regjeringen.no/no/om-regjeringa/slik-blir-norge-styrt/Regjeringa-i-arbeid/id2564958/

Regjeringen. (n.d., a). *Health and Care.* Retrieved April 20th 2020 from https://www.regjeringen.no/en/topics/health-and-care/id917/

Regjeringen. (n.d., b). *Norwegian Directorate of Health.* Retrieved April 20th 2020 from https://www.regjeringen.no/en/dep/hod/organisation-and-management-of-the-ministry-of-health-and-care-services/etater-og-virksomheter-under-helse--og-omsorgsdepartementet/Subordinate-institutions/the-directorate-for-health-and-social-af/id213297/

Regjeringen. (n.d., c). *Folkehelseinstituttet.* Retrieved April 20th 2020 from https://www.regjeringen.no/no/dep/hod/org/etater-og-virksomheter-under-helse--og-omsorgsdepartementet/underliggende-etater/folkehelseinstituttet/id213298/

Regulation (EU) 2016/679. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). Retrieved 30.04.2020 from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Schwalbe, K. (2019). *Information technology project management* (9th ed.). Boston: Cengage.

Shen, X., Dicker, A. P., Doyle, L., Showalter, T. N., Harrison, A. S., & DesHarnais, S. I. (2012). Pilot study of meaningful use of electronic health records in radiation oncology. *Journal of oncology practice*, *8*(4), 219-223.

Silverman, R. D. (2013). EHRs, EMRs, and health information technology: to meaningful use and beyond: a symposium introduction and overview. *Journal of Legal Medicine*, *34*(1), 1-6.

Sligo J., Gauld R., Roberts V. & Villa L. (2017). A literature review for large-scale health information system project planning, implementation and evaluation. *International Journal of Medical Informatics, 97,* 86-97. DOI: 10.1016/j.ijmedinf.2016.09.007

Speck, R. M., Weisberg, R. W., & Fleisher, L. A. (2015). Varying goals and approaches of innovation centers in academic health systems: a semistructured qualitative study. *Academic Medicine*, *90*(8), 1132-1136.

Swinkels I.C.S., Huygens M.W.J., Schoenmakers T.M., Nijeweme-D'Hollosy W.O., Velsen L.V., Vermeulen J., Schoone-Harmsen M., Jansen Y.J.F.M., Van Schayck O.C.P., Friele R., De Witte L. (2018). Lessons learned from a living lab on the broad adoption of eHealth in primary healthcare. *Journal of Medical Internet Research.* DOI: 10.2196/jmir.9110

Tamburri, D, A. (2020). Design principles for the General Data Protection Regulation (GDPR): A formal concept analysis and its evaluation. *Information Systems, 91,* 1-14. DOI: https://doi.org/10.1016/j.is.2019.101469

Tassey, G. 1995. "The functions of technology infrastructure in a competitive economy." Research Policy20(4): 345-362.

IT Governance Privacy Team. (2017). *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide - Second edition*. Ely, Cambridgeshire, United Kingdom: IT Governance Publishing. Retrieved April 30, 2020, from www.jstor.org/stable/j.ctt1trkk7x

Umble, E. J., Haft, R. R., & Umble, M. M. (2003). Enterprise resource planning: Implementation procedures and critical success factors. *European journal of operational research*, *146*(2), 241-257.

Vassilakopoulou, P., Grisot, M., & Aanestad, M. (2015). A frugal approach to novelty: patient-oriented digital health initiatives shaped by affordable losses and alliances. *ECIS 2015 Completed Research Paper,* 1-14. ISBN 978-3-00-050284-2

Voigt, P., & Von dem Bussche, A. (2017). The EU general data protection regulation (gdpr). *A Practical Guide, 1st Ed., Cham: Springer International Publishing*.

Yang, T. (2019). ICT technologies standards and protocols for active distribution network. In *Smart Power Distribution Systems* (pp. 205-230). Academic Press.

Yuan, B., & Li, J. (2019). The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation. *International journal of environmental research and public health*, *16*(6), 1070.

Zahra, S.A. and Covin, J.G. (1994), "The financial implications of fit between competitive strategy and innovation types and sources", The Journal of High Technology Management Research, Vol. 5 No. 2, pp. 183-211.

Øvrelid, E., & Bygstad, B. (2016, August). Extending e-health infrastructures with lightweight IT. In *Scandinavian Conference on Information Systems* (pp. 43-56). Springer, Cham.

Webster, J. & Watson, R, T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, *26*(2), 13-23.

10. Appendix

Appendix A: Interview guide

Table 10.1. Interview guide.

Candidate	
Date	
Attending the interview	
Preface (10min)	
Presentation of people attending the interview	
Information about anonymity. Permission to record the interview.	
Information about the purpose and the timeframe of the interview	
Questions for the candidate (40 min.)	
Personvern i helse pre-GDPR • For bedriften , oppfattes personvern i e-helse annerledes før og etter implementering av GDPR? • Kan du fortelle om noen typiske utfordringer organisasjonen hadde med personvern pre-gdpr? Føler du at Personvern på noen måte var en hindring for at helsefremmende initiativer kunne realiseres?	
IS helse-initiativer • Kan du fortelle meg om noen spesifikke projekter(helse informasjonsystem) som bedriften er involvert i • Har prosessen med initiativer endret seg på noen måte? • Noen IS-initiativer som har stoppet og hva var omstendighetene for det?	
Personvern post-gdpr • Fortell oss litt om prosessen organisasjonen gikk gjennom ved implementering av GDPR i personopplysningsloven. • Hvordan vil du beskrive overgangen? • Ref lover (pasientjornalloven, helseregister loven), hvordan oppleves samspillet mellom lovene som omhandler personlig helse data. • Med GDPR som lovgivende føring, føler du innovasjon på noen måte hindres? • Har GDPR "enablet" innovasjon kortsiktig/langsiktig?	
Samarbeid om behandlingsrettede helseregistre og felles dataansvar? • Hva er utfordringene? Endringer POST/PRE gdpr	
Vurdering av personvernkonsekvenser (DPIA) og ROS-analyse (risiko- og sårbarhetsanalyse) er verktøy/analyser som brukes innenfor e-helse. • Fortell om hvordan dere bruker det?	

• Tilstrekkelig? • Uklart?	
• Er bedriften involvert i noen prosjekter som benytter teknologier som ML/AI? • Hvilke utfordringer har dere møtt? • Hvilke tiltak gjøres for å løse utfordringer? Er lovverket modent nok for disse teknologiene innenfor helse?	

• Brownfield vs greenfield (installed base)
  • Er det problematisk med innovasjon som skal supplere allerede eksisterende løsninger/systemer?
  • Dataminimering
• Second-hand use of data	

• Compliance & trust o Grunnlaget for bruk av tjenester/produkter bygger på underliggende compliance. Hvordan bygger bedriften tillit til sine prosesser og produkter? Opplever dere at dere må vise mer enn bare GDPR-compliance for å kunne få solgt tjenester?	
• Føler du at GDPR (personvernforordningen) har styrket tilliten til digitale tjenester?	
Ending(10min)	
Time for questions from the interviewee	

Appendix B: Structured literature review, selected papers

Table 10.2. Results of literature search. From "Barriers in eHealth initiatives, a literature review", by F. Christensen and P. S. Næss, 2019, Unpublished manuscript, p. 9.

Title	Year published	Authors	Jounral/conference
Barriers and Facilitators to eHealth Use in Daily Practice: Perspectives of Patients and Professionals in Dermatology	2017	Ariens, L. F., Schussler-Raymakers, F. M., Frima, C., Flinterman, A., Hamminga E., Arents, B. W., Bruijnzeel-Koomen, C.A, de Bruin-Weller, M.S. & van Os-Medendorp	*Journal of Medical Internet Research*
Sustainable implementation of innovative, technology-based health care practices: A qualitative case study from stroke telemedicine	2018	Bagot, K., Moloczij, N., Barclay-Ross, K., Vu, M., Bladin, C. & Cadilhac, D	*Journal of Telemedicine and Telecare*
Integration of Health Care and Social Care by Technology	2017	Bierhoff, I., & Rijnen, W	*Handbook of Smart Homes, Health Care and Well-Being*
"Teleswallowing": A case study of remote swallowing assessment	2015	Bidmead, E., Reid, T., Marshall, A., & Southern, V	*Clinical Governance*
Process innovation meets digital infrastructure in a high-tech hospital	2017	Bygstad, B., Hanseth, O., Siebenherz, A. & Øvrelid, E	*25th European Conference on Information Systems (ECIS)*
The inertia of the status quo: A change management analysis of technological innovation	2014	Glascock, A. P.	*International Journal on Advances in Life Sciences*
Innovation Of, In, On Infrastructures: Articulating the role of architecture in Information infrastructure evolution	2014	Grisot, M., Hanseth, O. & Thorseng, A. A	*Journal of the Association for Information Systems*
Heterogeneous Inter-Organisational IT Innovation Creation: Institutional constraints in a public sector oriented market	2011	Hardless, C. & Jaffar, A	*Scandinavian Journal of Information Systems*
Physician's usage of mobile clinical applications in a community hospital: a longitudinal analysis of adoption behavior	2013	Hao, H., Padman, R. & Telang, R	*UK Academy for information systems Conference Proceedings*
Trends, Findings, and Opportunities: An Archival review of health information systems research in Nigeria	2017	Kenny, G., O'Connor, Y., Eze, E. & Heavin, C	*Journal of the Midwest Association for Information Systems*
Electronic health records: how can IS researchers contribute to transforming healthcare?	2016	Kohli, R., & Tan, S. S. L	*Mis Quarterly*
The eCollaborative: using a quality improvement collaborative to implement the National eHealth Record System in Australian primary care practices	2014	Knight, A. W., Szucs, C., Dhillon, M., Lembke, T., & Mitchell, C	*International journal for quality in health care*
Transforming operating rooms: factors for successful implementations of new medical equipment	2018	Misser, N. S., Jaspers, J., van Zaane, B., Gooszen, H. & Versendaal, J	*BLED eConference 2018 Proceedings*
Pilot study of meaningful use of electronic health records in radiation oncology	2012	Shen, X., Dicker, A. P., Doyle, L., Showalter, T. N., Harrison, A. S., & DesHarnais, S. I	*Journal of oncology practice*
A literature review for large-scale health information system project planning, implementation and evaluation	2017	Sligo J., Gauld R., Roberts V. & Villa L	*International Journal of Medical Informatics*
Varying goals and approaches of innovation centers in academic health systems: a semistructured qualitative study	2015	Speck, R. M., Weisberg, R. W., & Fleisher, L. A	*Academic Medicine*
Healthcare Information Systems (HIS) Assimilation Theory	2018	Sulaiman, H., & Wickramasinghe	*Theories to Inform Superior Health Informatics Research and Practice*
Lessons learned from a living lab on the broad adoption of eHealth in primary health care	2018	Swinkels I.C.S., Huygens M.W.J., Schoenmakers T.M., Nijeweme-D'Hollosy W.O., Velsen L.V.,	*Journal of Medical Internet Research*
Catalyzing healthcare transformation with digital health: Performance indicators and lessons learned from a Digital Health Innovation Group	2018	Tseng, J., Samagh, S., Fraser, D., & Landman, A. B	*Healthcare*
A frugal approach to novelty: patient-oriented digital health initiatives shaped by affordable losses and alliances	2015	Vassilakopoulou, P., Grisot, M., & Aanestad, M	*ECIS 2015 Completed Research Paper*