

Analysing Information Security amidst the Implementation of Implantable Medical Devices in Norwegian Healthcare:

Information Security through the Lens of Contradiction Management

STEFFEN TENDVALL ABRAHAMSEN

SUPERVISOR

Wael Soliman

University of Agder, 2024

Faculty of Engineering and Science

Department of Information Systems

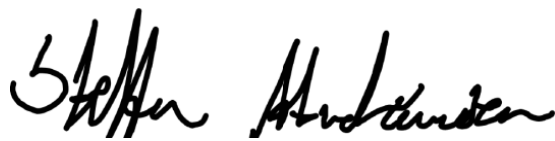
Acknowledgements

First and foremost, I would like to express gratitude to the thesis supervisor Associate Professor Wael Soliman of the Department of Information Systems at the University of Agder. Without the academic guidance and feedback, this endeavour would not be possible. I am deeply grateful for your help and sincerely appreciate it!

Secondly, I would like to thank all the interview participants. Your willingness to share your experiences and insight, along with the time you dedicated to this process. Without you sharing your knowledge this research would not be possible, thank you!

Lastly, I would like to sincerely thank my family, friends, and significant other for their support and encouragement throughout the years of study and during the process of writing the master's thesis. I am deeply grateful for that!

Kristiansand,
June 7th, 2024

A handwritten signature in black ink, reading "Steffen Abrahamsen". The signature is written in a cursive style with a horizontal line underneath.

Steffen Tendvall Abrahamsen

Abstract

Implantable medical devices (IMDs) are an electronic medical device that is implanted partly or within a human body to treat and monitor medical conditions. Modern IMDs have more computing power and are more interconnected. The use of IMDs have been very beneficial for effective patient treatment for the healthcare and have improved the quality of life for the users. Though IMDs being truly beneficial, it also comes with a cost. More computing power and interconnectivity leads to vulnerabilities and cybersecurity risks. Research have identified serious security and privacy risks in the use of IMDs and have expressed serious concerns. This thesis takes a new research approach to analyse and understand the environment IMDs are used.

This research analyses information security for the implementation process of IMDs in the Norwegian healthcare. Based on the collected data, resulted in a focus on insulin pumps and continuous glucose monitoring (CGM) domain of IMDs. The research uses the lens of contradiction management for the implementation of IMDs. Using process theory and stage modelling to build a stage-model to enrich the understanding of the implementation process. Using the stage-model and contradictions management if was possible to identify when and where challenges for implementation occur and see how they are solved. The goal of this research approach was to research the domain of IMDs from a new perspective. Potential revealing new insights and confirm or contrary existing literature.

The result discovered several contradictions that was solved during the implementation. The contradictions main topics was data storage and processing, information security and use of CGM applications. Implications showed that contradictions solved related directly to healthcare and end-users had a tendency to have lower information security outcome that strictly "IT"-contradictions. The findings also correlated with the literature of privacy concerns and the complexity of environment IMDs are used make is hard to apply effective theoretical information security and cybersecurity solutions.

Raising cybersecurity awareness for stakeholders for IMDs can help improve the information security and cybersecurity. Assist manufactures, healthcare personnel, patients and end-users to take educated choices to reduces unwanted information security and cybersecurity incidents. Regulations influenced choices during implementation, and future improvements in regulations can potentially lead to enhancing information security and cybersecurity for IMDs. The thesis concluding continuous research and work in the domain will enhance the information security and cybersecurity for IMDs.

Contents

- INTRODUCTION..... 1**
- 1.1 RESEARCH QUESTION 2
- 1.2 RATIONALE AND MOTIVATION 2
- 1.3 RESEARCH APPROACH..... 2
- 1.4 STRUCTURE OF THE THESIS 3
- BACKGROUND AND RELATED WORK..... 4**
- 2.1 LITERATURE REVIEW 4
 - 2.1.1 *Methodology*..... 4
 - 2.1.2 *Search for the Literature* 5
 - 2.1.3 *Screening & Quality Assessment*..... 6
 - 2.1.4 *Extract & Analyse Data* 7
- 2.2 LITERATURE FINDINGS..... 7
 - 2.2.1 *Implantable Medical Devices* 7
 - 2.2.2 *Types and usage of IMDs* 7
 - 2.2.3 *Vulnerabilities* 8
 - 2.2.4 *Cyber attack*..... 9
 - 2.2.5 *Security for IMDs*..... 9
- 2.3 LAWS, REGULATIONS, AND STANDARDS 11
- 2.4 INSULIN PUMPS AND CONTINUOUS GLUCOSE MONITORING 12
 - 2.4.1 *Insulin Pumps and CGM Complications* 12
 - 2.4.2 *Recall* 13
 - 2.4.3 *Privacy Concerns*..... 13
 - 2.4.4 *Terms of Service and Privacy Policy* 14
- 2.5 RESEARCH FOR IMDs 15
- 2.6 THEORETICAL LENS OF CONTRADICTION MANAGEMENT 16
- 2.7 SUMMARY..... 17
- RESEARCH APPROACH..... 18**
- 3.1 QUALITATIVE APPROACH..... 18
- 3.2 RESEARCH DESIGN 19
- 3.3 THEORETICAL LENS OF CONTRADICTION MANAGEMENT 19
- 3.4 PROCESS THEORY AND STAGE MODEL 19
- 3.5 DATA COLLECTION 20
 - 3.5.1 *Interview Process*..... 20
 - 3.5.2 *Interview Limitations* 21
- 3.6 DATA ANALYSIS 22
- 3.7 ETHICAL CONSIDERATIONS..... 23
- FINDINGS 24**
- 4.1 CONTRADICTIONS FOUR-STAGE MODEL..... 24
- 4.2 THE ORGANISATIONAL STRUCTURE OF THE HEALTHCARE SECTOR..... 26
- 4.3 STAKEHOLDERS 26

4.3.1	<i>User</i>	26
4.3.2	<i>Hospital</i>	27
4.3.3	<i>Sykehuspartner</i>	28
4.3.4	<i>Sykehusinnkj�p</i>	28
4.3.5	<i>Vendor</i>	29
4.4	STAGES AND CONTRADICTIONS	29
4.4.1	<i>Stage 1 Acquiring new Equipment</i>	30
4.4.1.1	<i>Data Storage</i>	31
4.4.1.2	<i>Training-data</i>	32
4.4.1.3	<i>Specific demands</i>	32
4.4.2	<i>Stage 2 Integration</i>	33
4.4.2.1	<i>Information Security Details</i>	33
4.4.2.2	<i>Third-party Application</i>	34
4.4.3	<i>Stage 3 Deployment</i>	35
4.4.3.1	<i>Device Selection</i>	35
4.4.3.2	<i>Data Processing and Storage</i>	36
4.4.4	<i>Stage 4 Use</i>	38
4.4.4.1	<i>Third-party Applications</i>	38
4.4.4.2	<i>Training-data</i>	40
4.5	SUMMARY OF CONTRADICTIONS.....	40
DISCUSSION		43
5.1	THEORETICAL IMPLICATIONS	43
5.1.1	<i>Laws, Regulations and Standards</i>	44
5.1.2	<i>IMDs environment</i>	44
5.1.3	<i>Third-party Application</i>	44
5.1.4	<i>Users' needs</i>	45
5.2	PRACTICAL IMPLICATIONS.....	45
5.2.1	<i>Cooperation</i>	46
5.2.2	<i>Cybersecurity awareness</i>	46
5.2.3	<i>Regulations and standards</i>	46
5.3	FUTURE WORK	47
5.4	LIMITATIONS.....	47
CONCLUSION.....		49
BIBLIOGRAPHY		50
APPENDIX A INTERVIEW GUIDE.....		53
APPENDIX B CONSENT FORM.....		54

List of Figures

Figure 2-1: The process of a systematic literature review (Xiao and Watson, 2019).....	4
Figure 2-2: Literature review	6
Figure 4-1: Contradiction Four-Stage Model.....	25

List of Tables

Table 2. 1: Table of keywords	5
Table 3. 1 Table of the interviewees.....	21
Table 4. 1: Summary of Contradictions.....	41
Table 4. 2: Summary of Contradictions (Continued)	42

Chapter 1

Introduction

The technology advancements the past decades have changed and improved medical treatment tremendously. Important factor for the increased capacity and capability for improved patient care is the interconnectivity between medical devices and clinical systems (Williams & Woodward, 2015). The healthcare industry in the US consumes over 15% of gross domestic product (GDP). Because of the rapid integration of smart devices for healthcare delivery, medical device becoming a huge part of this industry. By 2025 the global medical device market is expected to reach an estimated \$409,5 billion (Kwarteng & Cebe, 2022).

The rise of Internet of Things has influenced modern medical equipment. Small modern medical devices contain embedded computers system with powerful processing powers and the ability to communicate wirelessly through networks. A set of medical devices known as Implantable Medical Devices (IMDs) have experienced significant development and benefited from this technology (Alexander et al. 2019). IMDs is an electronic medical device that are implanted partly or within a human body. The devices help to treat medical conditions, by monitoring, improving functions of some body part, or provide patients with capability they did not possess before. Examples of such devices are pacemakers and defibrillators to treat cardiac conditions, neurostimulators to treat conditions as epilepsy or Parkinson, drug delivery systems as infusion pumps, and devices that monitor bio signals (Camara et al. 2015).

The increased and improved medical treatment with modern IMDs, have also come with a great cost. As the devices becomes smarter and more interconnected, the threat landscape also changes. Combined with a huge increase in cyberattacks targeting the healthcare sector the recent years, is this a very bad combination (Wilner et al. 2022). More computing power and wireless connectivity increase the possibilities for vulnerabilities and creates a much larger attack surface. Many researchers express concerns about this, as the devices store and process sensitive medical information, and perform medical treatment. There have been proven cases where some devices can be hacked, potentially causing harm to users or, in the worst-case scenario, being lethal. Cybersecurity encompasses a collection tools and resources as policies, security safeguards, risk management, best practises, to secure booth the devices and the privacy and safety for patients using IMDs (Alexander et al. 2019).

Cybersecurity and the health sector are where two different worlds emerged in modern times. Health care providers are in a difficult position regarding privacy and security protections. They are experts in science and medicine, not technologist or legal experts (Britton & Britton-Colonnese, 2017). Senior physician Torkel Steen has expressed concerns regarding privacy policies and patient safety in Norway. He emphasises that sharing patient information to monitor and improve treatment and safety is important. However, creating registries for patients with IMDs, such as pacemakers and defibrillators, has proven to be difficult to establish in Norway, and not in other countries. Steen's concern is that strict privacy regulations may interfere for patient safety (Steen, 2020).

1.1 Research Question

Given the complexity of stakeholders involved in medical equipment, exploring the lifecycle of implantable medical devices within the healthcare sector is a compelling topic. Investigating how information security is managed through the framework of contradiction management can provide valuable insights into operational practices. With this in mind, the following research questions are posed:

What are the information security contradictions encountered during the implementation stages of Implantable Medical Devices and how are they solved?

1.2 Rationale and motivation

This research aims to investigate the how information security is compiled with during the implementation of IMDs in the Norwegian healthcare. Following the lifecycle for IMDs, from they are acquired to the devices end of life. This is a timely interesting topic due several factors. Recent years there have been an increasing amount of cyberattacks against the healthcare sector, and smarter and more interconnected IMDs creating a bigger attack surface. The increased use of technologies in health care, understanding and integrating healthcare and cybersecurity can enhance patient treatment and safety.

Existing research explores IMDs from various perspectives; however, from existing literature, there has been no research conducted on IMDs through the lens of contradiction management. Researching through the lens of contradiction management can highlight aspects of information security that are done correctly and identify areas that may need to be addressed and changed.

1.3 Research Approach

The research approach has been through qualitative research to identify information security contradictions and how they are solved during implementation of IMDs. Using semi-structured interviews to gather information and data, and code the data to generate and create an overview over the contradiction identified throughout the implementation stages. The research started with a literature review of information security regarding IMDs create an understanding of the topic. Supportive and relevant literature for this research topic has also been utilized. During the period from February and April 2024, “11” interviews were conducted with individuals from the Norwegian Healthcare in the region of south-east, users of IMDs and vendor for IMDs. Through the interview process and the interviewee expertise, the research was tailored to focus on insulin pump and continuous glucose monitoring devices and systems. A subset of the interviewees contacted for a second time for more follow-up questions and all interviewees were reached out to confirm the data gathered from them. Coding the data and examining it through the lens of contradiction management contributing to answering the research question.

1.4 Structure of the thesis

Chapter 1 – Introduction:

Brief introduction to IMDs and information security challenges related to the topic. Rationale and motivation to conduct this research, and short description of the research approach.

Chapter 2 – Background and Related Work:

Explain the literature review process and present literature findings to create understanding for this research.

Chapter 3 – Research Approach:

Present the research approach, and reasoning chosen method. Show the process conducting the research and how data is collected. The methods for analysing the data for the findings.

Chapter 4 – Findings:

Elaborate the findings into different categories to help to identify contradictions.

Chapter 5 – Discussion:

Information accumulation of the finding of different categories. Present a summary of the finding. Discuss the findings from the literature review and interpreting the results. Discuss future work and limitations on the research.

Chapter 6 – Conclusion:

Conclusion on of the thesis.

Chapter 2

Background and Related Work

This chapter will present the literature review process and the findings to give an understanding of the information security and cyber security knowledge of IMDs. Discuss the methodology for literature review, including the search process for relevant literature and the screening process. The quality assessment criteria, then the data extraction and data analysis. This chapter will also give a brief introduction to insulin pumps and continuous glucose monitoring systems to show the correlation with IMDs.

2.1 Literature Review

Conducting a literature review before academic work is strongly beneficial. Building a comprehensive understanding and overview of existing literature, can foster theory development, identifies gaps in existing research, and uncover areas where more research is needed aiding to advancing knowledge (Webster & Watson, 2002).

2.1.1 Methodology

The methodology for the literature review is based on steps from Xiao & Watson (2019) paper on “*Guidance on Conducting a Systematic Literature Review*” as illustrated below. Following the steps of “Search for the literature”, “Screen for inclusion”, “Assess quality”, “Extract data”, and “Analyze and synthesize data” before final step of report and present the findings.

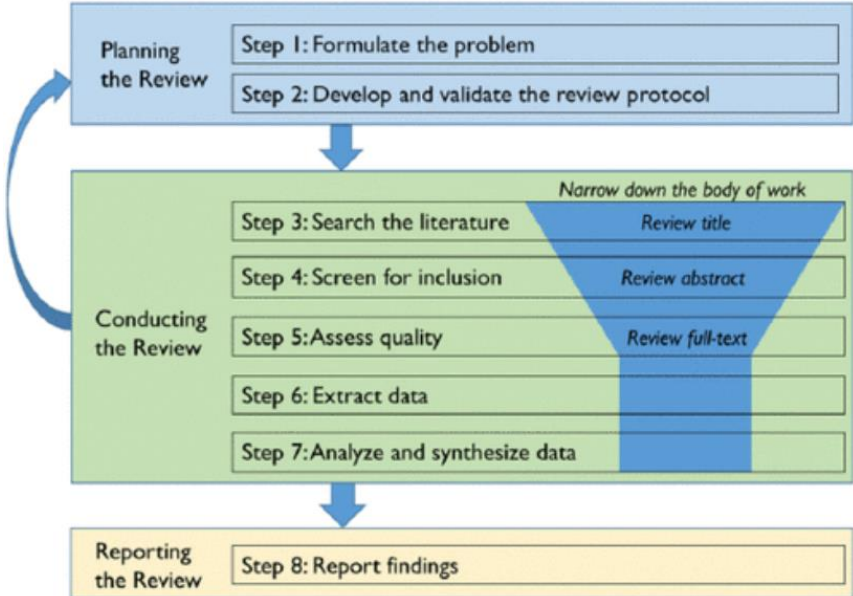


Figure 2-1: The process of a systematic literature review (Xiao and Watson, 2019)

2.1.2 Search for the Literature

To ensure a high standard of the literature review, it is important to make sure the literature used holds a certain quality. Electronic databases for published material are a good way to start, but ensure the search cover more publications more than one database should be used. The technique of “backward search”, find literature that has been cited by the article, and “forward search”, see literature that have cited the article, will assist further to obtain a more complete list of relevant literature. Keywords for the search can be derived from the research question domain, and further altered to get more relevant results. When the search has stopped given new information, that can be considered as a sensible stopping rule for the search (Xiao & Watson, 2019).

For the literature review the database “Web of Science” and “Google Scholar” has been used. The method of back- and forward search has been useful to snowballing the search. Keywords for the search is listed in *table x*. The search has also been conducted with abbreviations of the keywords and combining different keywords as “IMDs + Cybersecurity”.

Keyword for search	
• Implantable Medical Devices	• IMDs
• Information Security	• Cybersecurity
• Hacking	• Vulnerabilities
• Privacy	• Patient Safety
• Insulin pumps and CGM	• Healthcare

Table 2. 1: Table of keywords

Enhancing the quality and to assist to find relevant literature an inclusion criteria was created. The following literature review criteria was set for search:

- Literature written in English or Norwegian.
- Literature published between 2015-2024.
- Literature found through the search, snowballing, or referred by relevant informants.
- Literature should be peer-reviewed.

Argument for English or Norwegian is due for the research to be understandable. Reason for gather literature from 2015-2024 is that there commonly known for fast changes in technology and older literature might be outdated. Looking through research citations is an effective methodology to find more relevant literature. Lastly, literature that is peer-reviewed give an extra credibility to the literature.

The website “Register Over Vitenskapelige Publiseringsskanaler” has been used for an extra quality check as well as the site grade scientific journals to be trustworthy or not. Cautious when reading and using “grey literature” and lower quality literature as they might not fully trusted.

2.1.3 Screening & Quality Assessment

The screening process is a method to look through all the literature found in the first step of the search. Reading the abstracts of the literature and remove the literature not found relevant. When doubt if it is relevant, it should be kept for now. For quality assessment full texts reviews and remove the ones not relevant. A method to help ranking the quality assessment, is to rank the quality and relevance into “high”, “medium”, and “low”. Were high-quality can be used in the literature review, and medium and low can used more as supplement and not too foundational (Xiao & Watson, 2019).

The screening process started by looking on the titles from the search for literature. The total number of 62 articles were reduced to 36. Next step of the screening was reading the abstract, and removing the literature that was not relevant. Last step was the full-text review, 6 articles were removed, but due to snowballing 3 was added after the screening. *See figure 2.2.*

The final step was the quality assessment, where the literature was added in to three different quality ratings, “high”, “medium”, and “low”. This ranking worked as a guidance on the last quality and relevance of the literature for the research.

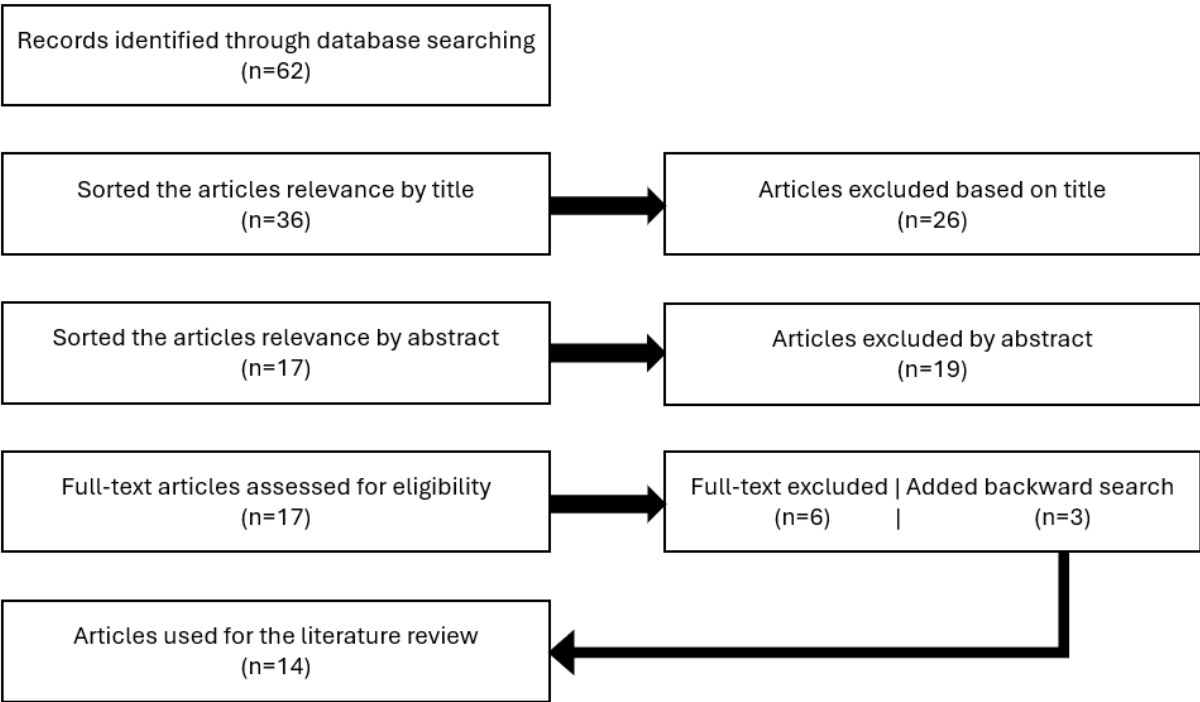


Figure 2-2: Literature review

2.1.4 Extract & Analyse Data

Following the steps of Xiao & Watson (2019) extracting data has been done through coding. Here the data was organized into relevant tables with supporting textual description. Example looking into data stored on IMDs, a table used for “pacemakers” and “privacy details” supported by textual description of privacy details on this device. After the extracting and analysing the literature, helped identify relevant finding for this research.

2.2 Literature Findings

This section will give a thorough introduction to Implantable Medical Devices. Explaining various types of IMDs and their unique applications, as well as explaining challenges related to information security. Including both cybersecurity and privacy challenges, and in the context these devices are used. The objective of this literature review is to enhance the understanding of the use of IMDs and to gain insight why the research in this thesis was conducted and potentially providing new insights and knowledge.

2.2.1 Implantable Medical Devices

Implantable Medical Devices (IMDs) are defined as a medical device that are either partly or totally surgically or medical implemented into the human body, for longer or shorter periods of time (Joung, 2013). IMDs functions is to address a medical condition, oversee physiological states, enhance the functionality of a specific body part, or offer the patient a new capability they previously did not have (Camara et al. 2015).

Modern IMDs are integrated with advancements in microelectromechanical systems technology with chemical-biological and mechanical expertise. Since this devices interface with the body is it crucial the body is not adversely affected by them. IMDs ability to wirelessly to be controlled and transmitting monitored patient data is essential, but also good for evaluating battery status and enhancing functionality. Most implantable devices come with equipped with a battery, biocompatible materials, and programmable circuits (Balas & Pal, 2020, p. 200). Along with the processing powers and wireless communication, IMDs also store sensitive information like vital signals, diagnosed condition, therapies, and a variety of personal data such as birth date, name and other medically relevant identifiers (Camara et al. 2015).

2.2.2 Types and usage of IMDs

IMDs improve the quality of life for users, and in some cases play an important role to keep the users alive. Common examples of IMDs are pacemakers and defibrillator for monitoring and treat cardiac conditions, neurostimulators for deep brain stimulation for conditions like epilepsy or Parkinson disease, infusion pumps for drug delivery, and various biosensors designed to read and analyse different bio signals (Camara et al. 2015). Another technology is electronic tattoos, elastic on the skin that can monitor bio signals. Most common are devices that are attached by strap- or tape-based to the human body (Balas & Pal, 2020, p. 201).

IMDs represents a great advancement in the field of medicine. As the devices give advantages for treatment of medical conditions. IMDs can help to control and monitor patients for a wide

range of diseases mentioned as diabetes, Parkinsons, and cardiac arrhythmia. As the devices automatically are programmed to administer some necessary treatments for the patients. The interconnectivity of IMDs and the monitoring functionality give the ability to a fulfil healing and diagnostic in a quick and cost-effective manner. Doctors can administer and help with advanced treatments to patients remotely through the use of these wireless interfaces while being physically away from the patients (Hassija et al. 2021). IMDs have improved the lives of millions globally. Continuing expanding the range and improved quality of IMDs treating more disorders with increasing efficacy (Pycroft & Aziz, 2018).

The advancements of medical equipment and improved treatment of medical conditions is also a great part of the medical industry. The US healthcare industry covers over 15% of the gross domestic product (GDP). As the healthcare uses more and more integrated technologies, by 2025 the global medical devices market is expected to reach an estimated \$409,5 billion (Kwarteng & Cebe, 2022).

2.2.3 Vulnerabilities

The recent technical advances in health care have increased the capacity and capability to improve patient care. One major factor is the increased interconnectivity between medical systems and other clinical systems. The interconnected of medical devices exposes them to security breaches similarly to other networked computing systems. However, unlike typical networked computing systems, there is a growing concern that this connectivity could have a direct impact on clinical care and patient safety (Williams & Woodward, 2015).

Multiple studies have consistently highlighted the advanced technology devices and interconnectivity also make them vulnerable for cybersecurity vulnerabilities and an increased attack surface. For instance, Hassija et al. (2021) emphasises the advanced IMD technologies will improve the quality of life for the users; on the other hand, they are exposed to an increased surface area for security attacks. Alexander et al. (2019) corroborate that the improved patient care of devices connected to the network may put patients at risk for cybersecurity vulnerabilities that are related to information and device function security. Siddiqi et al. (2018) underscores this by noting, though greatly advantageous for medical treatment; the wireless capabilities make it possible for malicious entities to communicate with the device. This increased attack surface can lead to several serious issues as private data theft, misdiagnosis, and physical harm.

Furthermore, the extensive range systems and parties that modern IMDs are connected to increase the attack surface. Extensive range of authorised users including programmers, administrators, patients, and physicians broaden the potential attack surface for IMDs. The increased attack surface present numerous challenges, and the rise in ransomware attack within healthcare sector has introduced additional risks for IMDs (Kwarteng & Cebe, 2022).

2.2.4 Cyber attack

So far, there are no known real-world incidents where a user of IMDs have been attacked. But several attacks have been successfully demonstrated in laboratories (Camara, 2015). Various research group have explored and demonstrated security attacks to show open vulnerabilities of IMDs. Although there are no real-life incidents for security breaches on IMDs, the demonstration is realistic and can potentially put patient lives at risk (Hassija et al. 2021).

Types of attacks are related to which device that is hacked. Implantable cardioverter defibrillator and pacemaker devices was proven to be hacked in 2017 and 2018, where the hacker was able to perform a battery drain attack and depleting the battery, resulting in reduced lifespan for the device. Also, the devices could be reprogrammed or corrupt the program to send irregular and improper pacing and shocks, potentially could be lethal. Neurostimulator was hacked in 2018 by a group of Belgian security researchers. They found a loophole to unauthenticated and unencrypted messages. The loophole allowed the hacker to deliver electrical shocks, obtain sensitive neurological and medical information. In 2011 hacking of an insulin pump was demonstrated, the attack made the pump deliver a fatal dose of insulin. Though this hack was demonstrated in 2011, the risks relating such attacks should not be ignored at present times (Hassija et al. 2021).

Siddiqi et al. (2018) conducted a threat-modelling analysis based on attack trees to evaluate some security aspects of IMDs. An attacker can either be an outsider or an insider with different security privileges. From there assumed an attacker's aim is to prevent patient treatment, perform data manipulation, or steal private patient data. Following the process of the attack tree there are different paths to how an attacker potentially can gain authorised access and perform the hacks that have been demonstrated.

Improving security approaches and techniques, understanding of attackers' motivation could be helpful. Attackers' motivation can be physical harm, vicious groups could threaten, hurt, or kill patients. Monetary goals, inflict damage to competitors, such incident could influence the stock market. Privacy breach, collect sensitive data from users of IMDs. Tracking, some devices send patient-specific health and location data, receiving and eavesdropping the signals can potentially track the movement of a patient (Hassija et al. 2021).

2.2.5 Security for IMDs

Cybersecurity is crucial for digital transformation. Increasing and evolving threats makes cybersecurity important for public safety. The importance of IMDs for patients lives, makes the ensuring security high priority for IMDs manufactures and healthcare providers (Kwarten & Cebe, 2022). Cybersecurity can be defined as:

“Cybersecurity is a broad term that encompasses the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and an organization and user's assets.” (Alexander et al. 2019, as cited in ISO/IEC 27032:2012(E)).

Ensuring cybersecurity for IMDs is of high priority. Studies have shown to mitigate risk for IMDs, using known information security and cybersecurity practices will enhance the security. Follow security regulations and standard will also improve the security of medical devices. IMDs have a different goal than normal embedded systems, but vulnerabilities discovered in the domain of IMDs are common cybersecurity vulnerabilities. Usage of common practices and aspects of CIA triad will help to ensure security (Kwarteng & Cebe, 2022).

Using the basic model of confidentiality, integrity, and availability, known as “CIA triad”, can help to improve the security of IMDs. Showing common basics of cybersecurity have an importance of securing medical devices. Kwarteng & Cebe (2022) elaborates the following:

Confidentiality in IMDs:

Communication among IMDs, programmers, remote controls, hospital systems, and manufacturers involves sensitive data that must be protected from unauthorized access. This includes patient information, health records, device status, usage data, monitoring logs, audit trails, and user behaviour data. Ensuring confidentiality during data transfer and storage is crucial to prevent breaches by hackers or malicious actors.

Integrity in IMDs:

Ensuring the integrity of data exchanged between IMDs and their programming or remote servers is vital. The accuracy and authenticity of this data are essential for providing correct and effective patient therapy and treatment. Any compromise in data integrity can negatively impact the quality of healthcare provided to patients.

Availability in IMDs:

IMDs must provide continuous monitoring or stimulation for treatment. They need to be accessible for patient therapy and for physicians to make adjustments. Ensuring availability includes defending against denial-of-service attacks that could deplete device resources, thereby ensuring consistent and reliable treatment delivery.

From the development and design, it is practically impossible to create a perfectly secure IMDs, as with any other computer system. And trade-offs between security and functionality for IMDs will always be a factor. Collaboration between manufacturers, physicians, security researchers and regulators to focus on developing secure devices and maintain good security practices when the IMDs are being used (Pycroft & Aziz, 2018).

Hassija et al. (2021) mention audit process to ensure security. Auditing helps to prevent and detect if there are any security attacks. Due to limited memory of IMDs, use of external device with no memory limitations should be used for auditing purposes. Williams & Woodward (2015) have also concluded that auditing should be an operational practice and be able to report to the governance lever of an organisation. Lack immediately reporting and recognition of cyber security incidents is problematic. Camara et al. (2015) suggest more standard cybersecurity practices as access control and cryptographic measures.

Williams & Woodward (2015) states that effective risk management and regulatory compliance are crucial for patient safety, particularly regarding networked medical devices. Governance processes should document data flows to ensure protection during data transfer, processing, and

storage. They express the issue that current risk management frameworks often overlook these devices and their vulnerabilities, as they are typically managed by biomedical technicians, not IT departments.

Although following all best practices for cybersecurity to secure IMDs are effective from a theoretical view. As IMDs are a computer system implanted in a human body, there is no guarantee that a patient will follow all guidance for cybersecurity. Studies designing security considering the patients point of view could potentially be beneficial to enhance security (Camara et al. 2015).

2.3 Laws, regulations, and standards

The acknowledgment of cybersecurity as a critical vulnerability in medical devices has prompted regulatory authorities to assist and provide guidance. Both in the US and European Union laws and regulations for pre-market submission and post-market surveillance. The most notable authority is the Food and Drug Administration (FDA), giving recommendations for managing cybersecurity risk to safeguard patients and data, created and processed by medical devices (Williams & Woodward, 2015). In Europe the most prominent regulation is the General Data Protection Regulation (GDPR). GDPR covers data protection and privacy in the European Economic Area (EEA). Individual countries often enforce their own national regulations for sensitive data in addition to GDPR, which are especially regarding to the medical field (Randine et al. 2023).

While the GDPR governs data transfers within the EEA, there are concerns about transferring personal data to countries outside this area. The Schrems II case brought attention to these issues and led to the invalidation of the Privacy Shield in 2020. This shield was a self-certification used by US companies to comply with GDPR standards. As a response, the European Commission proposed Standard Contractual Clauses to regulate data transfers from the EU to entities outside this jurisdiction not bound by GDPR regulations. Information about data transfer in Europe must be made available for users or patients through the Terms of Service (ToS) and Privacy Policy documents provided by data processors (Randine et al. 2023).

IMDs, being medical devices, generate, accept, use, store, manipulate, and transfer patients' health and personal information. Because of this IMDs are in the US subjected to follow the Health Insurance Portability and Accountability Act (HIPAA) regulations for privacy rules and guidelines. Furthermore, the security of IMDs is rigorously governed by the FDA under the FDA Regulation of Medical Devices Act. As a result, manufacturers are required to adhere to both pre-market and post-market policies (Kwarteng & Cebe, 2022).

In EU the two regulations of Medical Device Regulation (MDR) and In Vitro Diagnostic Regulation (IVDR) assist to govern medical devices in Europe. In Europe a medical device is defined by MDR as a device that designed to diagnose, prevent, monitor, predict, prognosis, or treat disease. From 2026 the European Database on Medical Devices (EUDAMED) will be mandatory with goal to facilitate traceability, cooperation and transparency within the medical sector. For now, it is voluntarily if a vendor wants to register devise in the EUDMED database (Randine et al. 2023).

Standards offer trustworthy best practices. There are several international standards are prerequisites for certification of medical devices. As many security flaws and vulnerabilities is a result of poor software design. Standards for development and design risk assessment is important. Providing good practices in the lifecycle of risk and development process (Williams & Woodward, 2015).

2.4 Insulin Pumps and Continuous Glucose Monitoring

Both insulin pumps and continuous glucose monitoring (CGM) systems are often categorized as types of implantable medical devices, despite not always requiring surgical implantation in the conventional sense. Insulin pumps function by continuously delivering insulin to the body, usually via a small catheter inserted beneath the skin. Although the pump itself is not surgically implanted, the accompanying infusion set, which includes the catheter, is inserted into the subcutaneous tissue and remains in place for several days. This setup qualifies insulin pumps as a type of implantable device. Similarly, CGM systems involve inserting a small sensor beneath the skin, typically on the abdomen or upper arm, to monitor glucose levels in the interstitial fluid throughout the day. While the sensor is not permanently implanted, it remains in place for a specific period, usually ranging from several days to a week, before requiring replacement (Domingo-Lopez et al., 2022). Future generation of devices will be more implantable versions, where research and testing are in progress (Kropff et al., 2017).

CGM help users from harm of low blood sugars, known as hypoglycaemia. CGM alarms alert the used when glucose level has fallen below a threshold that it determined unsafe. Some diabetes patients may have hypoglycaemia unawareness, where the body do not give signals as shakiness or sweating to low blood sugars, and CGM alerts are crucial. Using networked CGM linking various devices as smartphones or computers using applications. They can send data to the applications; users can see their information for analysis and identify trends without removing the devices from their body. Easy access to the data can further enhance the understanding of diabetes. Some apps can deliver personalised messages in real time, helping to track food intake and help to understand event how specific actions or habits affect their glucose levels (Britton & Britton-Colonnese, 2017). While smartphones and extra third-party applications are not strictly necessary, they are helpful to facilitate monitoring and automatic data recording and data transfer to managing diabetes. Users that do not want to use this applications alternative will be provided (Randine et al. 2023).

2.4.1 Insulin Pumps and CGM Complications

Healthcare providers have a responsibility to "do no harm" and should inform patients about technologies, products, and services that can improve their health. Currently, advanced and sufficient regulatory landscape, it is challenging for healthcare providers to recommend correct use of CGM. Healthcare providers are experts in medicine and science, not in technology or law. Therefore, they find it hard to recommend products without fully understanding and explaining the potential impacts on a patient's privacy and security when all risks are not adequately addressed (Britton & Britton-Colonnese, 2017).

The CGM medical devices and software applications are widely used in patient treatment. The primary used of the data is for plan for treatment for patients. However, some of the applications

used are not directly integrated into the Electronic Health Record (EHR) systems. This creates a challenge for healthcare providers that must use multiple systems with different logins and platforms. This can consume valuable consultation time and potentially impact patient care quality. Moreover, it is important to understand that this CGM-applications and system are not meant to be integrated with the EHR-systems. As they are not designed to or do not aim to replace EHR. Example the “LibreView” data management systems decelerate is not an EHR-system and must bring the information deemed relevant by the users themselves for medical treatment (Randine et al. 2023).

2.4.2 Recall

There has been recall for IMDs devices such as cardiac implants before. One case recall was cardiac pacemakers recalled in 2017 from the brand Abbott. FDA issued a voluntary recall for the 465, 000 devices spread over six different models. The devices were given a firmware update to fix a vulnerability that gave unauthorised access. Use of the unauthorised access could potentially disrupt the normal operation for the device or perform a battery drain attack (Hassija et al. 2021). The first recall of devices related to diabetes devices was in 2019. The devices that were affected by the recall was Medtronic insulin pumps that were on the market before 2013. This was a historic decision because it is the first time a manufacturer had recalled a diabetes device for cybersecurity vulnerabilities. FDA announced the warning or patients and healthcare providers. There was also an incident in 2016 where a flaw in insulin was discovered. The brand Animas handled the incident well through cooperating with a cybersecurity company through coordinated vulnerability disclosure. (Klonoff & Han, 2019).

For a healthcare professional it was important to explain to the patients that exploiting the vulnerability would require considerable skill from a hacker. The FDA also reminded the importance of wireless technology and software offer safer, more convenient and timely health care delivery. Though a recall is newer good news, awareness around a recall would hopefully lead patients, healthcare providers, deice manufacturers, and the FDA, increase their effort to that diabetes devices will meet and withhold established security baselines in design and through the products lifecycle (Klonoff & Han, 2019).

2.4.3 Privacy Concerns

Currently it is a grey area for laws and regulations for CGM-applications. In the US, HIPAA are privacy and security rules to protect protected health information (PHI). These regulations are for health care professionals, insurers, and certain business associates. HIPAA enforces strong data privacy and security protections for patients and provide safeguarding to protect patient information. In short, the HIPAA privacy rules give a patient right over their own information such health information and records. Then patients can on the own choosing to forward this information to any person or entity, such as a phone application. Applications for CGM provide customers with their privacy policy, and users agree, CGM-applications are not legally obligated to follow the strict HIPAA regulations, though store and process the same sensitive health information (Britton & Britton-Colonnese, 2017).

The Federal Trade Commission (FTC) oversees how entities handle person health information, especially when users manage medications from device like CGM. A breach of unsecured health information, the FTC requires that affected users, the media, and the FTC itself shall be notified. The FDA oversees apps used for diagnosing or treating diseases to ensure safety and accuracy. If an app poses minimal risk, the FDA might not enforce strict regulations. For example, apps that help users manage their health by tracking data like blood glucose levels or diet without suggesting treatments usually do not face strict regulation. However, if an app uses attachments to measure blood glucose levels, it is considered a "mobile medical app," and the FDA will apply regulatory oversight. Such apps, like those turning a phone into a glucose meter, must meet safety and effectiveness standards before being sold (Britton & Britton-Colonnese, 2017). A complex landscape for jurisdictions creates a grey area for some devices and systems operate in. Overall, there a still measures from authorities to secure CGM-applications.

Research conducted on Terms of Service (ToS) and Privacy Policy documents of diabetes medical equipment and software applications approved of use in Norway. Of the 11 identified medical equipment, only three of them was registered in EUDAMED. And none of the 12 software applications were registered. Though this can be a result the requirements for registration in EUDAMED to fulfil MDR and IVDR regulations are not before 2026. These findings highlight the importance of focusing more on ensuring regulatory compliance and enhancing data-sharing practices in diabetes management (Randine et al. 2023).

2.4.4 Terms of Service and Privacy Policy

Privacy concerns arise with CGM manufacturers and associated apps storing and sharing patients' health data without clear guidelines or oversight on adequate protections. Users often lack information about how their data is used and have little control over it. For instance, Dexcom's privacy policy collects various user data but lacks specifics on how personal information is deidentified. Privacy policies can change without warning, leaving users unsure about data security. There is a pressing need for stronger safeguards in data collection, storage, and sharing, as even deidentified information can potentially be reidentified. Both patients and healthcare providers need to be mindful of the less apparent risks associated with CGM and similar technologies, which can expose them to privacy breaches. Until stronger privacy and security safeguards are implemented, patients will have to determine their own comfort level regarding the associated risks to their privacy and security when using these technologies (Britton & Britton-Colonnese, 2017).

Randine et al. (2023) conducted a thorough document analysis of Terms of Service and privacy policy documents regarding the regulation of data sharing for diabetes medical equipment and associated software approved by the Norwegian healthcare authorities. The findings indicated that the development of medical device technology is primarily led by companies based outside the EU. And ToS and privacy policy documents are very difficult to understand for end users. They require high level of legal and digital literacy to be understood. Resulting in most users may not understand what they are agreeing to when accepting the ToS. For the 12 software applications used for diabetes data transfer and analysis the compliance for GDPR security requirements varied. 8 out of 12 were relying on adequacy decisions and the last 4 did not.

Terms of Service and Privacy documents of diabetes medical device are shown to be difficult for ordinary users to comprehend and demand a high level of legal and digital knowledge. Due to the complex and legal language, many users may agree to these terms and conditions giving consent without understanding them. As the dilemma for users the benefits of using applications outweighs the challenges of navigating lengthy ToS documents. Some the document for applications also lacks comprehensive information regarding data processing and storage, or techniques for de-identification, encryption protocols, and data format. Once accepted to the ToS and data is shared with an application there is a chance the provider or the patient, no longer control the data use, access, or disclosure (Randine et al. 2023).

2.5 Research for IMDs

We now have a better understanding of the complexity revolving IMDs. The following section presents an overview of the research findings from the literature. Examining the existing studies help to highlight the current state of IMDs and underscore the need for ongoing effort to enhance the safety and security of medical devices.

Williams & Woodward (2015) researched the complex environment they are used in. As IMDs are connected to the network, resulting in tension between security and safety, and how this is not only a technical problem as that there is subsequent contention between regulation and manufacture. Looking into examples to highlight the diversity of the cybersecurity challenges. In a health care setting, patient safety will always come before cybersecurity requirements. Since medical devices and medical networks now are more important for patient treatment than ever before, the challenge to close the gap between the two objectives becomes really important. This will require increased collaboration between medical physicist, IT professionals and manufacturers to enhance cybersecurity. They also discover the need for cybersecurity protection must be integrated into the design and development of medical devices. Updated standards and national guidance are addressing these needs, along with establishing accountability for medical device cybersecurity through standards and regulatory oversight. Advocacy from the medical device industry is crucial to promote greater awareness of cybersecurity and privacy issues.

Camara et al. (2015) comprehensive survey for security and privacy issues for IMDs concluded collaboration among experts in manufacturing, bioengineering, and computer security is vital to ensure patient safety and data privacy. Despite some effective theoretical security solutions, the IMDs are faced with practical implementation challenges, and it is unclear what the optimal choice would be. Responsible usage and increased security awareness among users and medical personnel are necessary is a key for success. Kwarteng & Cebe (2022) did a survey of the IMDs domain and aimed to address not yet solved security problems. The survey highlighted the growing number of IMDs on the market and the need for enhanced security measures as they advance technologically. Despite the benefits and market growth, cyber-attacks on IMDs are rising, emphasizing the importance of proactive security to protect patient privacy.

Siddiqi et al. (2018) had a different research approach. Using an attack-tree-based threat for IMDs to create an expanded reference point for the research. The approach offered a comprehensive and highly structured view over the strength and weaknesses for IMD systems. The approach allowed for new insights that could help to improve security. Example providing

a structured approach for performing system-level security evaluation to include as many attacks surfaces as possible.

As the consensus of the literature show concerns regarding cybersecurity for IMDs. Hassija et al. (2021) explored and researched if the security concerns for IMDs are exaggerations or represent actual security threats manufacturers and users should be concerned about. Although no real-world breaches have occurred, research shows vulnerabilities that could endanger patients. Confirming the existing concerns for IMDs and recommend further suggested thorough research and improvement of security aspects in the design, development, installation, and usage of these devices can enhance patient confidence in adopting these medical solutions.

2.6 Theoretical Lens of Contradiction Management

In organisational theory contradiction is a well know phenomena. Earlier pioneering studies addressed tensions such as organisational effectiveness and employee welfare, and newer studies cover a wide range of topics related to organisational contradictions (Hargrave & Van de Ven, 2016). To define contradiction the following citation will be used:

“Contradictions are defined as dynamic tensions between opposite elements that together form a unity and logically presuppose each other for their very existence and meanings” (Werner & Baxter, 1994, as cited in Hargrave & Van De Ven, 2016)

Contradictions are often researched through two different lenses, paradox, and dialectical perspectives. Paradox focusses on the contradiction where the tension of two opposite elements is ongoing and coexist. While the dialectical perspective is that tension equilibrium is impossible to coexist. Resulting the contradiction to one of the opposite elements to give way for the other, or some cases producing new transformation or solutions. The process can be identified as, the affirmation, when two opposite elements engage. The negation, the contradiction releasing the tension between the elements and produces a way forward, the transformation. (Hargrave & Van de Ven, 2016).

The lens of contradiction management has been used to help to understand information security complications in existing literature. Niemimaa & Niemimaa (2019) researched the approach an innovative engineering company developed and established they information security policies. The process of implementing their security policies the management of a top-down or bottom-up approach. The study included contradiction management to help to explore the tensions during the process. Soliman & Ojalainen (2023) had similar approach in conflict resolution during the implementation of information security ISO/IEC 27001 standard. Use of contradiction assisted to give insights of the main tension for the implementation process the ISO standard. Demonstrating the use of the lens of contradiction management can give valuable insights in the domain of information security and cybersecurity.

2.7 Summary

There are clear medical benefits for patient treatment with use of IMDs. Researchers have expressed cybersecurity concerns for the devices. As the evidently have been proven to be hackable, and the consequence of a cyber-attack would be severe. The environment for IMDs, from production and usage has shown to be very complex. Laws, regulations and standards aim to improve cybersecurity, privacy and safety in the use of IMDs. Despite the efforts, research there is need for more research to improve information security and cybersecurity for IMDs.

Following Siddiqi et al. (2018) new research approach for IMDs as they used attack-tree-based approach to in the hope to new scientific discoveries. Will this research use the approach of contradiction management to potentially offer a new view of cybersecurity challenges for IMDs. Potentially leading to new empirical finding that help to improve the cybersecurity, privacy and safety for patients using IMDs.

Chapter 3

Research Approach

This research objective is to identify and highlight contradictions for IMDs in the Norwegian health sector. From the phases of acquiring and buying new IMDs, how these devices and systems get integrated with today's ICT-structure, and when they are being taken in use and the usage of IMDs. To help address the objective of this research the following research question has been formulated:

What are the information security contradictions encountered during the implementation stages of Implantable Medical Devices and how are they solved?

The research focus on the healthcare sector of the southeast region of Norway, as most of the interviewees are from organisations belong to that region. This does not preclude the possibility that the research may be relevant to other regions in Norway or other countries. While conducting the research most of the interviewee had data related to insulin pumps and CGM. Which made the research approach alter from IMDs in general, to more specific research into insulin pumps and CGM.

This chapter present the method of choice for research approach. Explaining the research design and the use of contradiction management as a theoretical lens. Guiding through the data collection process, how the interviewee selected or introduced and detailing the process how interviews were conducted. Subsequently, it explains how the data were analysed, discusses the limitation of the analysis and the ethical considerations.

3.1 Qualitative Approach

The most distinctive feature of a qualitative approach is that it allows to identify issues from the study participants experience (Hennink et al. 2020). Whereas quantitative strategies focus on data as numbers, qualitative strategies focus on data as words. That gives qualitative method the potential to utilize basic principles as inductive analysis, where data is gathered first and then creates and build patterns, themes, and concepts into meaningful abstract of data. As well as a holistic and contextual approach, use the data to create a comprehensive and more detailed picture of a complex phenomenon. This approach typically helps to look at a phenomenon from multiple perspectives and develop a larger picture (Recker, 2021).

To be able to answer the research question there were several crucial factors for the qualitative approach. The datatype had to be qualitative to build an inductive understanding and an overview for the research case. More important to have the correct data to code it was crucial to get an insight and understanding the interviewee experience point of view. From the numbers of potential interviews that could be conducted it was sensible to go for a qualitative approach. Building up for the research it was also important the approach was somewhat agile to be able to return to the interviewee for follow up questions and gathering more data.

3.2 Research Design

Research design is to create a plan for the collection, measurements, and analysis of the data to help to answer the research question. The plan should be efficient while representing the decisions involved in the research planning, which often require balancing compromises and trade-offs among resources, time, quality, and data access (Recker, 2021).

First step underdoing this research was to get an understanding and overview over different segments and organisational are connected. The mentioned principle of inductive analysis has helped in this matter while analysing data during the entire process of the research. The choice of coding has also been enhancing for the contradiction management perspective.

3.3 Theoretical Lens of Contradiction Management

To help to gain new insights for IMDs, this research will be done through the theoretical lens of contradiction management. As contradictions are tension between two elements, using this lens on the implementation of IMDs in the Norwegian healthcare, this could give a better understanding for how information security challenges are solved. Identified contradictions show the challenge from the perspective from both of the opposing elements, this could possibly give better insights on a topic.

For this research an opposing element will be named through the stakeholders relating to IMDs and the implementation phase. The stakeholder will be identified as “A” and “B” in a identified contradiction where the stakeholders are working as opposing elements. The result of an identified contradiction will be marked as “A”, when “element A” prevail with its proposal, or result “B” when the result turned in “element B” proposal. Result “C” will be used when element “A” and “B” cooperate a new solution.

3.4 Process theory and Stage model

To help to understand the contradictions during implementation of IMDs in the Norwegian healthcare, the use of process theory and a stage model will be used.

Process studies investigate how and why things emerge, develop, grow, or terminate over time (Langley et al. 2013). Using a process study on the implementation of IMDs can help to give insights and understanding of the process. For contradictions is relevant to understand how two elements emerge and find a way forward. And an implementation is something that occur over a given period, this can be seen as an ongoing process.

Stage models can describe a wide variety of phenomena, such as the life cycles of organizations, products, and biological growth. These models create predictable patterns visualized in stages, such as the growth of organizations, sales levels of products, the diffusion of information technology, or the growth of living organisms. Stages are arranged in a sequential order, occur as a hierarchical progression that is not necessarily easy to reverse, and involve a broad range of activities and structures (Solli-Sæther & Gottschalk, 2010; King & Teo, 1997).

Process theory is more flexible and dynamic, capturing the complexity of real-world processes. It is useful for understanding how processes evolve over time and the factors influencing them. Stage models provide a structured framework that simplifies complex processes into manageable segments where phases can be identified. Incorporating these theories can help the research of implementation of IMDs to systematically understand and describe the lifecycle and deployment.

3.5 Data Collection

Qualitative research most prominent form gather data is through interviewing. Interviews have the advantage of targeting the focus on selected topics and allowing the interviewees to share their thoughts on cause and effect. While conducting the interview gives the control to use follow-up and probing questions to steer the conversation to certain areas of interest. Using semi-structured interviews is a solid tool for this. As semi-structured interviews usually start with a general question on the topic, but the follow-up questions are created out of the conversation and gives the flexibility to ask for further details or discuss other issues that seems more beneficial (Recker, 2021).

To back up the choice of qualitative approach using interviews was the obvious choice. Using semi-structured interviews were chosen since a topic for the questions relevant to the research questions was created beforehand the interviews. Keeping it semi-structured also gave the advantage to ask follow-up questions that was not prepared in forehand to discuss new occurring information.

Because of the diverse backgrounds of the interviewees, the semi-structured questions were rarely the same but were all derived from the same template, created with the research question in mind. Further on in the research questions was sometimes prelimited on gaps or needed clarification for gathering supporting data for the final data analysis.

3.5.1 Interview Process

As a collaboration with Sykehuspartner they assisted with potential and relevant sources within the organisation. Naturally to start researching for information and conducting interviews here. From there the list of potential individuals, both within Sykehuspartner and other organisation, that would be in my interest to reach out too started snowballing. All except two interviewees were contacted through this process.

The interviews were conducted over Teams besides for two, where one was one phone and the other physically. Each interview lasted from 30 minutes to 60 minutes. All interviewees were contacted at least twice regarding the data collection process. First contact was the conducting of the full-length interview. Second contact was to validate the data after some coding, ensuring that the data were correct, and give the potential to necessary corrections or deletions. Some of the informant had two full-length interviews to gather more information as the research progressed. Messages and mail were also used to clarify data and information.

Vendor and Hospitals is used as a pseudonym to anonymise the name of the medical equipment vendor and which hospital in the region of Helse Sør-Øst. The total number of interviewees is 11. An overview of the organisation and the participants background or title are listed in *table 3.1* with following number that identifies the interviewee.

Interviewee	Organisation	Participants
#1	Vendor	Advisory Board Vendor, Programme Lead DFIR
#2	Sykehusinnkjøp	Legal Specialist Advisor, Insulin pump & CGM
#3	Sykehuspartner	ICT Service Developer, Hospital-Specific Clinical Solutions
#4		ICT Advisor, System Designer
#5		Senior ICT Advisor, Risk Assessment
#6		Senior ICT Advisor, Security Advisory
#7	Hospital	Section leader, Diabetes
#8		Clinical Nurse Specialist
#9	User	CGM, IT & Technical Background
#10		CGM, IT & Technical Background
#11		CGM, Non-Technical Background

Table 3. 1 Table of the interviewees

3.5.2 Interview Limitations

Conducting qualitative interviews there are many pitfalls and difficulties that can occur (Myers & Newman, 2007). From Myers & Newman chapter over “Problems and pitfall” relevant limitations is explained:

- Lack of trust: As a stranger for the interviewee or the chance of holding back information that potentially could be consider too “sensitive”. Specially in this research touching on topic relevant to information security and health sector topics.
- Level of entry: To whom to contact and get in touch with interviewees in an organisation can be difficult, special as a researcher. For this case the “banner” from Sykehuspartner have helped reaching out to informants but should still be aware of the limitation.
- Constructing knowledge: Pitfall to be biased to information and create falls understanding or constructs. Though being cautions during the research, the risk will still be there. Specially since this research understanding were somewhat build up from scratch during concurrent data coding. Measurement to avoid this was continuous contact with some of the interviewees.
- Ambiguity of language: Words and terms might not be understood. This happened during the interviews, by being aware of this limitation clarifications were often asked for. This perhaps been extra relevant for this research due to different field of expertise from medical, law and IT.

3.6 Data Analysis

For data analysis in this research the method of coding has been used. Codes are mainly used to organize and group similar pieces of data. This helps the researchers quickly find and organize segments related to specific research questions or themes. By clustering and condensing these segments, researchers can then analyse them further and draw conclusions. Coding gives a deep reflection, deep analysis, and interpretations of the data's meaning (Miles et al., 2013).

It is also strongly recommended to analysis concurrent data during the research period. It helps to get an overview of existing data and generate good strategies for collecting new and often better data, and a good way to correct missed blind spot in the start of the data collecting (Miles et al., 2013). Analysing data along the way has been a good method for gaining an understanding and overview of the complexity for IMDs and stakeholders. With the use of principles of inductive analysis and a holistic and contextual approach. Once this overview was created, it can then be brought back to the interview subjects for confirmation or correction. Open the possibility to ask more questions building upon the already done research. While analysing the data the importance to be aware of the pitfall to too quickly name patterns and codes that could lead to wrong or poor understanding of the data.

The coding followed two stages, First Cycle and Second Cycle. First Cycle consist of up to 25 different approaches, each with different function or purpose. The different coding approaches can be mixed and matched as needed. Second Cycle is to group the data from First Cycle into a smaller number of categories, themes, or constructs. With the use of Pattern codes, it helps to pull the material from the First Cycle into more meaningful and concise units of analysis (Miles et al., 2013).

The coding methods are profiled from Miles et al. (2013) book "Qualitative Data Analysis".

First Cycle methods used is In Vivo coding, Process coding and Holistic coding. In Vivo Coding uses words or short phrases from the interviewee's own language. It helps to learn the correct terminology in the field of study and phrases repeated help to point out regularities or patterns for the given setting.

Process coding helps to understand actions the emerge, change, occur over time in particular sequences or become implemented. Building upon the process theory approach. By highlighting "-ing" words it can identify action, interaction, and consequences. Holistic coding method applies a single code to categorize a larger unit of data to make an overview before starting more detailed coding of the data. Giving the foundation for the stages by sorting relevant processes into categories of the implementation process.

Second Cycle methods used is Pattern codes, Network Display and to some extent Cross-Case Analysis. Pattern codes help to tie together bits of data, where patterns usually consist of four summarisers: 1. Categories or themes, 2 Causes/explanations, 3. Relationships among people, 4. Theoretical constructs. Network Display highlight data describes a process and show how over time things act or transform. Cross-Case Analysis aim to improve general applicability or transferability to different settings, mostly adapting data different research. In this case more used to understand and draw independent view from the different stakeholders.

Pattern coding was used to structure data into different categories and themes, reflecting where each process occurred. The identified implementation processes fit into four distinct categories, which could be termed stages of the implementation. Coding with a focus on Network Display and using a stage model research approach helped construct the stage model for the study. Process coding identified various processes within the data, and by combining pattern codes that highlighted relevant stakeholder relations, the stakeholders involved in each contradiction were identified. Cross-Case analysis approach provided a more comprehensive understanding of the intersection between healthcare and technology from an information security perspective, allowing for a more nuanced analysis of the issues at hand.

3.7 Ethical Considerations

All behaviours involved in a research process are subject to ethical considerations. Particularly ethics related to empirical data collection and human subjects. Honest and complete reporting of how the data is analysed and the result is important to represent. Even though the results may be negative or are undesired, or when they run against the premise of a paper or research design (Recker, 2021).

All interviewees were volunteers and had given their consent to use their information and data for this research. Everyone was contacted at least twice to be able to affirm, correct or ask to remove any data or statements, as well with the interviewee titles. The research project is applied and informed to Sikt, ensuring compliance for privacy and ethical data handling.

This research will not represent any sensitive data. Researching topic related to health sector, health data, patient information, and business secrets may be a silver lining. All organisations have given consent to use data for the research.

Chapter 4

Findings

To be able to answer the research question,

“What are the information security contradictions encountered during the implementation stages of Implantable Medical Devices and how are they solved?”,

there was a steep learning curve on how the Norwegian healthcare is interconnected. The research discovered multiple contradictions for the implementation of insulin pumps and CGM. Five main stakeholders have been identified. Researching the processes from acquiring new medical equipment throughout to the implementation and use, a four-stage model have been created. The four-stage model give an overview of the correlation between the contradictions and stakeholders throughout the implementation of insulin pumps and CGM.

4.1 Contradictions Four-Stage Model

To summarize the findings from the identified stakeholders and stages, a "four-stage model" has been created. The model helps explain and provides a clear overview of the processes and contradictions during the implementation of insulin pumps and CGM in the Norwegian healthcare sector.

The stages are numbered sequentially from left to right to illustrate the progression of implementation. Each stage illustrates a prominent step in the implementation process. Stakeholders involved in each stage are presented vertically. The model categorises the findings into distinct stages where stakeholders encounter contradictions inherent to the implementation process. Arrows in the model illustrate how stakeholders intervene during each stage. Contradictions are mapped to their respective stages and associated stakeholders, detailing the outcomes. Each stakeholder as an element for tension, is indicated with an “A” or “B”. The result from the contradiction is stated with “A”, when “element A” prevail or “B” when “element B” prevail their proposal. Result “C” states that element “A” and “B” have cooperated a new solution form the contradiction to move forward.

This approach enhances the understanding of how various stakeholders interact within each stage, highlighting the tensions and outcomes arising from these contradictions during the implementation of IMDs.

Further elaboration will be provided in the following section on contradictions. For the process to move forward to the next stage, the contradiction in the current stage needs to be resolved. The mode will work as guidance when reading the finding section.

Short summary of contradictions shown in table X in the end of the chapter.

Contradictions Four-Stage Model

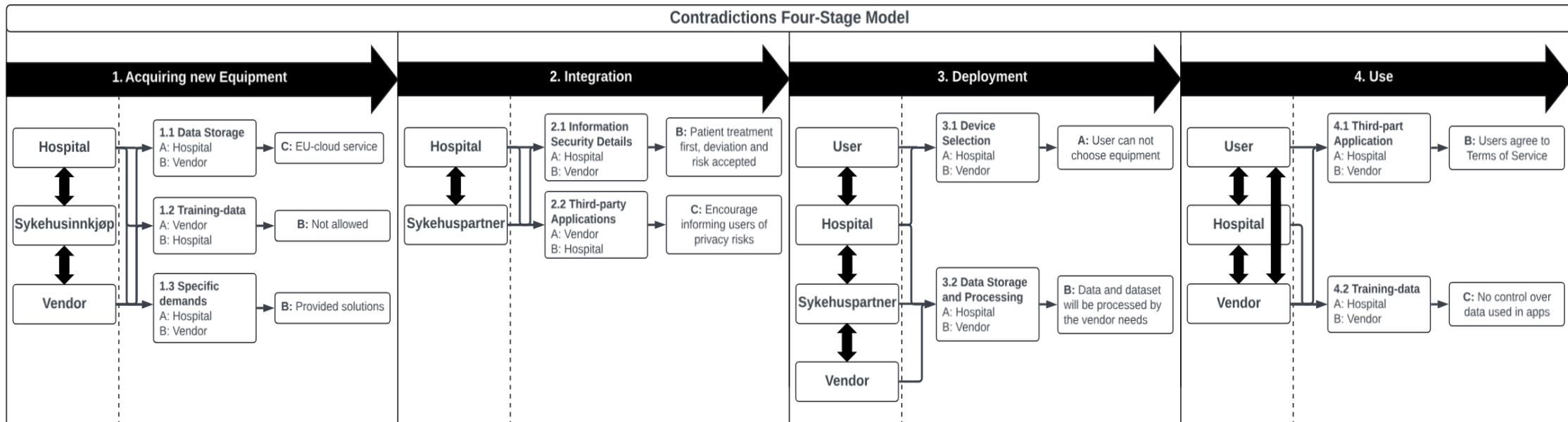


Figure 4-1: Contradiction Four-Stage Model

4.2 The organisational structure of the healthcare sector

To gain an understanding of how the research approach, how it is conducted and its complexity, it is also important to have a brief introduction to the structure of the healthcare sector in the southeastern part of Norway. In the following paragraphs highlight the overview of the structure, and organisations that are involved regarding IMDs equipment.

The state of Norway owns the healthcare sector in Norway, with the Ministry of Health and Care Services responsible for its administration. The regional health authorities are divided into four regions. Where each health authority is responsible for providing specialized healthcare services to the population in that region. They are also responsible for the public hospitals in the region, and the hospitals are organized into health trusts (Regjeringen, 2023).

Helse Sør-Øst RHF is responsible for the southeastern region of Norway. They are responsible for total of 11 health trust in the region, where 9 of them are hospitals delivering specialised treatment, the last two are Sykehusapotekene and Sykehuspartner (Helse Sør-Øst RHF, 2024). Sykehusapotekene own the pharmacies located on the hospitals in the region and aim to increase patient safety and cost related to medicine procurement for the health trusts and patients as low as possible (Sykehusapotekene, 2023). Sykehuspartner manage all information and communication technology systems for the hospitals. These are systems as clinical and administrative applications, ICT infrastructure, networks, and workspaces for 81.000 users (Sykehuspartner, 2024).

For acquiring new medical equipment and deliver the equipment there is two more organisations that is relevant for this research. Sykehusinnkjøp is owned by the four health regions of 25% each. Their task is to help the health trust create deals with vendors when procurement and acquiring new medical equipment. They are responsible for providing the best deals for new health equipment for the health trusts (Sykehusinnkjøp, 2024).

Behandlingshjelpemidler provide assistance for medical equipment used in medical home treatment for which the health trusts are responsible, but treatment or equipment is used outside of the hospitals itself (Nasjonal Nettverksgruppe for Behandlingshjelpemidler, 2024).

4.3 Stakeholders

There has been identified several stakeholders for the implementation stages of insulin pumps and CGM-systems. Some of the stakeholder was more obvious from the start in an information security and privacy point of view, but some occurred while learning and understanding more on how the Norwegian healthcare is interconnected. The stakeholders have been named in terms used to support the revealed contradictions. Therefore, some of the stakeholder terms are comprehensive terms and cover several organisational parts of the healthcare.

The five stakeholders are “User”, “Hospital”, “Sykehuspartner”, “Sykehusinnkjøp” and “Vendor”.

4.3.1 User

The stakeholder users are individuals that use IMDs. In this case insulin pumps and CGM-systems on daily basis to improve their quality of life. These are individuals that either has Type 1 or Type 2 diabetes. Though the term user in relevant studies also be used for health staff that use this equipment and systems in their work but for this research and finding it is out of scope.

Defining the stakeholder user was done through the interviews where the interviewee informed, they had one of the types of diabetes and explaining the usage of insulin pump and CGM devices in their daily life. Interviewee expressed:

“I feel much more freedom in daily life. Not having to carry insulin pens or anything visible on my body. It's discreet; no one can see it. Unlike with pens, which are noticeable and harder to hide.” [Interviewee #11, User]

Two interviewees expressed the utilisation of CGM functionalities:

“Glucose monitoring helps me regulate my energy levels throughout the workday and during training after work.” [Interviewee #9, User]

“While driving the use of CGM applications helps in planning for breaks.” [Interviewee #10, User]

As the individual clearly express usage of the devices and CGM-system. By being active users of IMDs devices, they also will have to be considered as a stakeholder.

4.3.2 Hospital

Hospital is the most complex stakeholder and owned by the south-east health region authorities. Hospital serves as an umbrella term for several health trusts in the southeast region. The hospital encompasses various department responsible for the operations within the hospital. For this research Behandlingshjelpemidler have been mentioned often, as they are responsible for the delivering, service, and end of life of medical equipment used outside hospitals.

“(…) in the diabetes sections we can assist in finding and facilitating the right equipment, but the agreement for the medical equipment is between Behandlingshjelpemidler and the patient.” [Interviewee #7, Hospital]

“(…) professional group may consist of specialists from Sykehuspartner, input and experiences from Behandlingshjelpemidler, and advisors from the Diabetesforbundet.” [Interviewee #2, Sykehusinnkjøp]

Understanding that Behandlingshjelpemidler as an organisation working within the hospitals and have lot of responsibility and expertise for medical equipment as insulin pumps and CGM. Additionally supporting the number of different departments and operations ongoing on a hospital the following was said:

“Hospitals have dedicated security personnel for completing PDA and DPIA.” [Interviewee #6, Sykehuspartner]

“(…) hospitals them self are responsible for booth security and cybersecurity themselves, we can advise, but they take the final decision.” [Interviewee #5, Sykehuspartner]

This demonstrates the complexity within hospitals, particularly in term of information security and Behandlingshjelpemidler role in handling medical equipment. Using “Hospital” as an umbrella term proved to be appropriate, due to the relevance of the contradictions in this research. Internally, hospitals also encompass various departments responsible for the

operations within the hospital. They are responsible for different specialized healthcare services, in this case the treatment of diabetes, is also a part of the stakeholder umbrella term.

4.3.3 Sykehuspartner

Sykehuspartner is also owned by the south-east health region authorities. Sykehuspartner is responsible to provide ICT for the health sector of the southeastern region of Norway. Defining Sykehuspartner to stand out as stand-alone stakeholder and not a part of hospital, is due it different responsible the stages compared to hospitals. To identify and defining Sykehuspartner role in the health and asking what Sykehuspartner role is, Senior ICT Advisor stated:

“We have little influence over what hospitals choose to purchase in terms of solutions, but we are here to support them in setting up and configuring the systems so that they have the access they need and can then use the systems on the healthcare network”. [Interviewee #6, Sykehuspartner]

Though the hospitals are accountable for information security themselves. Sykehuspartner job is to assist and inform the hospitals in ICT manners. When data is stored or processed in Sykehuspartner network, they are responsible to follow laws of data regulations. The interviewee from Sykehuspartner and another underscored this by stating:

“As one of our tasks is to perform risk analysis on new systems or system changes, this requires system documentation (...). (...) creates a document with the identified risk to inform the hospitals. (...) it is up to them whether they wish to accept the identified risks.” [Interviewee #5, Sykehuspartner]

“(...) data stored or processing by Sykehuspartner, it is crucial that we comply with regulations. We cannot enforce or do the job for the hospitals, but we can assist them in complying with the regulations.” [Interviewee #6, Sykehuspartner]

Discovering contradiction between hospitals and Sykehuspartner becomes relevant due to the tasks with assisting to adhering to the privacy laws and regulations and create system and risk analysis documentation for the hospitals. And since Sykehuspartner main objective is to assist the ICT structure, and not directly perform patient treatment as the hospital, they will be identified as individual stakeholder for the implementation process in Norway.

4.3.4 Sykehusinnkjøp

Sykehusinnkjøp is owned by all four health regions. Their objective is to support procurements processes when acquiring new medical equipment. Hospitals comes to them when on the need for acquiring new medical equipment. Clinical nurse said the following:

“Hospitals can make “smaller” medical purchases themselves without tender. Large purchases and projects must occasionally be put out to public tender.” [Interviewee #8, Hospital]

Legal Specialist Advisors confirming the same and said:

“(...)we assist in equipment procurement and offer expertise in both technical and legal matters. (...)facilitate negotiation and finalization of sale agreements.”
[Interviewee #2, Sykehusinnkjøp]

Sykehusinnkjøp play an important role to acquiring new medical equipment and is involved in the procurement of the new insulin pumps and CGM equipment. As their goal is to assist hospitals acquiring new medical equipment, their assistance is important of the success to solve some of the revealed contradictions. Assisting procurement of new medical equipment, advise from professional group Diabetesforbundet and experts from the hospitals and Sykehuspartner also support the process.

“(...) assistance from relevant expertise from the hospitals and Sykehuspartner. (...) for insulin pump and CGM, the Norwegian association for was also involved.”
[Interviewee #2, Sykehusinnkjøp]

Findings show that Sykehusinnkjøp appearing as a more neutral stakeholder and not directly as an opposing element. As for acquiring new medical equipment the work as a middleman to front the tension from the hospital and the vendor.

4.3.5 Vendor

Perhaps one of the obvious stakeholders and involvement in several contradictions. But due to the high number of different vendors involved delivering insulin pumps and CGM system the term “vendor” will be used an umbrella term to cover them all. Confirming the number of different vendors Senior ICT Advisor, RISK said:

“Obtaining all system documentation is challenging due to the involvement of multiple subcontractors.” [Interviewee #5, Sykehuspartner]

As the medical equipment contains various technical components from different suppliers, same for the IT-system solutions they are running on. And a variety of insulin pumps and CGM systems are bought and already in use. Legal Specialist Advisor said:

“This involves multiple suppliers, as insulin pumps and CGM systems consist of various components.” [Interviewee #2, Sykehusinnkjøp]

Clinical nurse says:

“There are many different solutions for diabetes patients can use, but ultimately, the different equipment accomplishes the same task.” [Interviewee #8, Hospital]

As the involvement from a high number of vendors in the lifecycle of insulin pumps and CGM-system, the term vendor will be used to cover the entire supply chain.

4.4 Stages and Contradictions

This section will present the findings used to create the stage model for the contradictions. The contradictions were placed in identified stages throughout the implementation process. Each discovered contradictions for stage, needed to be solved for the process to move to the next stage. For a contradiction to exist, there needs to be tension between two stakeholders. The

discovered contradictions will be presented in the occurring stage, with a stage number and a sub-number for each individual contradiction. Followed by a description for the resolution of the contradiction. Contradictions for each stage will be summarised in a table at the end of the findings section.

Four stages were identified, the four-stages are “1. Acquiring new Equipment”, “2. Integration”, “3. Deployment”, and “4. Usage”.

First glance there would be natural with a fifth stage as well, end of life or after use, but no contradictions were discovered relevant to this topic. As Sykehuspartner and Hospital stated:

“(…) service or repairing, there are routines to not ship them with privacy details on the shipment.” [Interviewee #8, Hospital]

“Behandlingshjelpemidler is required to have procedures when equipment is no longer used, in place to ensure that privacy details are not compromised.”
[Interviewee #3, Sykehuspartner]

Showing that for this research there were no need for a “end of life” stage understanding routines were in place and no relevant contradictions were revealed.

4.4.1 Stage 1 Acquiring new Equipment

The first stage during the implementation is the stage how the Norwegian healthcare acquire new medical equipment such as IMDs. Already stated that large purchases need to be done thorough public tender. The last procurement has been a public tender, the agreements have also been published public. Latest procurement has also been a national wide procurement for all health regions, and is supported by this statement:

“(…) procurement of new insulin pumps and CGM equipment has been national, encompassing all health regions with support from Sykehusinnkjøp.” [Interviewee #7, Hospital]

To establish a start for the stage of acquiring new equipment, information about how the hospital bought new medical equipment identified the start of the process. Following statements talked about the topic:

“The hospital comes to us when they want to buy medical equipment, (…)”
[Interviewee #2, Sykehusinnkjøp]

“Large purchases and projects must occasionally be put out to public tender. (…). When we have decided the need to buy something, the hospital reach out to Sykehusinnkjøp.” [Interviewee #8, Hospital]

As the hospitals have decided the need for new equipment, the evidence show it is when the hospital identified a need the ball starts rolling, and they contact Sykehusinnkjøp. Some of the discovered contradictions were highly relevant for the procurement for insulin pumps and CGM and placed in the stage 1.

4.4.1.1 Data Storage

One major topic for acquiring new insulin pumps and CGM where is data going to be stored. To move forward with an agreement, this had to be solved. Hospitals, as the Norwegian healthcare, first suggested to be able store the data on their own systems in Norway. This would not be possible because of how the medical product and system solutions worked, and it would require too much configuration to function. Sykehusinnkjøp and vendor stated:

“(...) hospitals wanted to store and process data locally, or in their own infrastructure.” [Interviewee #2, Sykehusinnkjøp]

“(...) not possible to send a product and be done with it. (...) There is a need to be able to patch and update a system. (...) we are legally obligated to monitor the medical solutions we deliver.” [Interviewee #1, Vendor]

As the majority of vendors are American based companies, they would prefer to store data in the US. This was not a term the Norwegian health sector could agree to. Due to strict EU data protection laws, such as GDPR and the outcome of Schrems II. The data processor agreement for patient data in the Norwegian hospitals also states that data should preferably not leave EU. This is what Sykehuspartner, and hospital said on the topic:

“(...) and other companies delivering CGM systems are US based, and often prefer information management locally.” [Interviewee #5, Sykehuspartner]

“The ruling of the Schrems II also made it more difficult for US based firm to store data over there. (...) solution to the problem is the use of EU based cloud services.” [Interviewee #5, Sykehuspartner]

“Sending patient data abroad, is normally not allowed for our systems.” [Interviewee #7, Hospital]

With the assistance of Sykehusinnkjøp in the negotiations, a common ground was reached to use data storage within the EU. The contradiction would not stay long as a stalemate, as it is common for the Norwegian healthcare to use EU cloud services for such solutions. Asking for what are done in similar practices:

“More and more solutions use cloud services that are based in EU.” [Interviewee #4, Sykehuspartner]

“Some data will always end up in the US, but using EU servers is a common thing.” [Interviewee #1, Vendor]

Resolution for the contradiction was the use of EU-cloud data storage. Option of store data locally for the hospital would never be an option since, as the insulin pumps and CGM-system would take too much configuration to be possible. On the other hand, American vendors could have stood their ground more and kept the data on their system in the US. The progress of laws and regulations as GDPR and the result of Schrems II it has become a more common practice for the American companies to use EU-based cloud services.

The topic of data storage and data processing will reoccur in stage 3.

4.4.1.2 Training-data

During the procurement process, the vendor expressed a desire to access anonymised user data sourced from Norwegian patients. Their intention was to leverage this data to enhance the quality and performance of their products, aiming for continuous improvement based on real-world usage insights.

“One segment was about the vendors wanted training data from us.” [Interviewee #7, Hospital]

“Vendors do often want anonymised training data to improve their products.” [Interviewee #3, Sykehuspartner]

However, in adherence to standard data processing agreements for Norwegian patient data and governing privacy laws, the requests cannot be allowed. Asking how they solve this request:

“Our hospitals DPA do not allow data to be used as training data, only for some research with consent from the patients. (...) Norway’s small population we do not see the big impact for manufacturers anyways.” [Interviewee #8, Hospital]

“It is common for the hospitals to no share data for training purposes.” [Interviewee #6, Sykehuspartner]

Contradiction was easily resolved by the Norwegian healthcare had no interest providing the vendors with training-data and the vendors accepted these terms.

The topic of training data will reoccur in stage 4.

4.4.1.3 Specific demands

One last contradiction discovered during stage 1 involved negotiations with vendors. There was a limit to how specific the Norwegian healthcare system could be with its demands regarding information security and functionality adaptations. The vendors indicated that excessive customization would make delivery impossible.

“The vendors’ feedback was that too much customisation and configuration would make delivery impossible.” [Interviewee #2, Sykehusinnkjøp]

This was confirmed to be more an issue of the return on investment in the production of medical equipment, rather than a lack of willingness to cooperate, as the vendor stated:

“It’s about the return on investment in the research and production of equipment, which is a costly process.” [Interviewee #1, Vendor]

“It is easier to make adjustments for larger countries like Germany and the UK than for Norway. (...) products delivered to Norway are of the same quality and functionality as those provided to other nations.” [Interviewee #1, Vendor]

As stated, this means that the medical equipment provided to the Norwegian healthcare is still provided with the same quality of equipment as other nations. Contradiction resolved by instead of the vendors having to adapt and customise their products for the Norwegian healthcare, the

Norwegian healthcare must adapt to the solutions offered for insulin pumps and CGM by the vendors in certain aspects.

4.4.2 Stage 2 Integration

As an agreement is done for acquiring the new insulin pumps and CGM, ending stage 1 and start the next stage. There is a need to integrate the bought systems to the already existing healthcare network and systems. Sykehuspartner is responsible for the ICT services for the region. Statement to help identifying Sykehuspartner as a stakeholder, is repeated here:

“We have little influence over what hospitals choose to purchase in terms of solutions, but we are here to support them in setting up and configuring the systems so that they have the access they need and can then use the systems on the healthcare network”. [Interviewee #6, Sykehuspartner]

As the ICT provider it is their role to provide the necessary documentation to booth Sykehuspartner and the hospitals for correct information system management. Asking about the reasoning for provide documentation, it was stated:

“Undergoing risk analysis on new system and system changes is required by laws and regulations, most known example is “Normen”.” [Interviewee #5, Sykehuspartner]

The integration stage is completed when the stakeholders agree the necessary documentation are in place. Defining agrees the necessary documentation, it is when the hospitals are satisfied and informed about the risk presented from the risk analysis. Senior ICR Advisor said the following:

“We can advise on measurements to reduces the risk, but it is up to the hospital if they want to go through with them, it is up to them whether they wish to accept the identified risks.” [Interviewee #6, Sykehuspartner]

Finalising the integration stage, and the next configuration is ready to be deployed.

4.4.2.1 Information Security Details

When procurement is completed, the hospitals contacts Sykehuspartner to find a way to integrate the new solution into the existing healthcare network. The contradiction emerging here is related to information security management. Sykehuspartner informed:

“We have little influence over what hospitals choose to purchase in terms of solutions (...) we can encourage the purchase of solutions implemented by other hospitals, so that parts of the work can be reused to reduce costs. Ultimately, however, it is the hospitals themselves that decide what to purchase.” [Interviewee #6, Sykehuspartner]

For information security management there a lot of documentation that needs to be gathered and properly documented. Complete documentation is need to booth the progress to integrate

to the existing network and solutions, and to have a complete risk assessment and information security governance.

“As one of our tasks is to perform risk analysis on new systems or system changes, this requires system documentation (...).” [Interviewee #5, Sykehuspartner]

“Undergoing risk analysis on new system and system changes is required by laws and regulations, most known example is “Normen”.” [Interviewee #5, Sykehuspartner]

“Obtaining all system documentation is challenging due to the involvement of multiple subcontractors.” [Interviewee #4, Sykehuspartner]

To understand the process, asking more questions about the system documentation and risk assessment. And what are the challenges related to this topic.

“We do our best to gather full documentation, (...) missing documentation or high risks involved, treatment for patients always comes first. (...) continuous work or measurements can be done at later stages.” [Interviewee #5, Sykehuspartner]

“For risks identified, we document them in the risk assessment. Where it is possible, we suggest measurements to reduce identified risks. (...) is the hospital themselves that will need to accept the risks.” [Interviewee #6, Sykehuspartner]

“Need for medical equipment and IT for patients (...), patient treatment always comes first.” [Interviewee #8, Hospital]

Understanding the process between Sykehuspartner and hospital, it is the hospital in the end must accept and own the risks identified. Where either would be missing documentation or high risk evolved leading to incomplete information security management, the need for medical equipment and system will be accepted, as the need for patient treatment always comes first. Accepting risks on medical equipment that is need urgent, do not mean the work for information security is completed and it can be an ongoing process.

In general, the contradiction between the hospital and Sykehuspartner regarding incomplete information security management, patient treatment always comes first.

4.4.2.2 Third-party Application

Sykehuspartner have identified a privacy risk related to use of third-party applications that can be connected to the insulin pumps and CGM systems. Third-party applications are applications that do not originally belong to the “closed loop” of the CGM system delivered by the hospital but can be downloaded by users at their discretion. As the use of these applications the users get access to some more functionals booth on applications on smartphones and widgets on smartwatches. Sykehuspartner expressed concerns related to privacy using third-party apps are that the data processed in these apps occurs outside Sykehuspartner network, and Sykehuspartner no longer has control over the data. Contradiction occurred from this is that Sykehuspartner would like to enforce users not to use the applications.

Data processed in third-party applications are beyond our control, as these applications operate outside our infrastructure. [Interviewee #3, Sykehuspartner]

Inform about the consequences of using apps and advise against them. [Interviewee #5, Sykehuspartner]

The reasoning behind this becoming a contradiction is the tension as the hospital cannot enforce and deny users of insulin pumps and CGM-system what to do. The hospital is aware of the privacy concerns, and they said:

We are aware of the issue, but we cannot dictate what the patients choose to do.
[Interviewee #8, Hospital]

From an information security perspective, ideally, these applications should not be permitted, but Sykehuspartner cannot enforce this regulation on the hospitals. As the hospitals cannot enforce what patients do after they have received their insulin pump and CGM equipment. Resulting in a middle ground that Sykehuspartner would like the hospitals to inform the user about the privacy concerns so users can take a more informed decision.

The topic of third-party applications will reoccur in stage 4.

4.4.3 Stage 3 Deployment

As the plan for integration is completed, the deployment stage starts. Stage 3 encompasses two identified primary events. The first being where patients receive their medical equipment. Asking users about the process of getting equipment they stated:

“I had nothing with the process of selecting new equipment. The hospital called me when the insulin pump was ready to be picked up.” [Interviewee #9, User]

“Only called in for a meeting to get the pump and CGM equipment, and information for the equipment.” [Interviewee #11, User]

Though users not showing to have an active part of process to receive equipment, for them get the equipment from the hospital is part of the deployment stage.

Second, it where the intricate IT system for insulin pump and CGM goes live. The new systems documented and designed and are prepared to be integrated to the existing network and establish access to the vendors digital product.

“(…) planning and completing the necessary documentation, next is implementation into our infrastructure.” [Interviewee #4, Sykehuspartner]

This is an important part of the deployment of insulin pumps and CGM as this very everything gets fully interconnected and systems goes live.

4.4.3.1 Device Selection

A contradiction related to device selection was discovered, it was shown that users had little to no input of choosing their own diabetes medical devices. To understand the equipment procurement process for a user, the hospitals explained:

“The healthcare provider and the patient discuss to identify the needs, after which the most affordable option that meets those needs is provided.” [Interviewee #3, Hospital]

Following up by asking if the user has any input on the selection of equipment or if they have expressed any cyber security or privacy concerns about the equipment they receive:

“No, the users have no say in what equipment they receive. The only reason to change medical equipment would be to medical reasons.” [Interviewee #8, Hospital]

“The most common requests are related to design or colour, based on research they have done on some models themselves. The sceptics are often those who work with computers.” [Interviewee #7, Hospital]

Interviewing users they explained it the same way. The equipment is delivered from Behandlingshjelpemidler, and the most cost-effective and suitable device is delivered. Asking if they had any cyber security or privacy concerns:

“Generally, functionality is more important than security on such devices, but had I been aware of major risks, I would have refused.” [Interviewee #10, User]

“I was aware of some minor vulnerabilities, but also aware that I couldn't ask for the device I actually wanted anyways.” [Interviewee #9, User]

“Overall, I really don't care to much about, I trust the process and the hospitals have routines for this.” [Interviewee #11, User]

Getting new medical equipment only reason for a user to be able to change is due to medical reasons. Giving the users to ask or order the equipment they would prefer. Further exploring this contradiction and the reason behind this practice, hospitals stated that:

“Procurements involve functional, technical, and cybersecurity clarifications to ensure patients receive quality equipment. This process is costly and time-consuming and would have been much more expensive if patients were given free choice of equipment.” [Interviewee #8, Hospital]

The result of the contradiction is that the users have no say when getting insulin pumps and CGM-systems. It would not matter if they would have information security concerns or simply not like the design of the equipment. The users only have minor concerns about cybersecurity but understanding the procurement process both functionality and cybersecurity have been a topic that should be covered.

4.4.3.2 Data Processing and Storage

The topic for data storage reoccurs at this contradiction. This contradiction primarily concerns the practical use of data storage and the processing and transfer of data, rather than the specific location and method of storing the main data. For when the systems of insulin pumps and CGM are deployed for use. There are some practical complications that arise. The agreement where

data should be stored was settled by using EU cloud-services keep the data within EU. A part of the data transfer challenge Sykehuspartner expressed:

“A lot of medical equipment is produced by American companies, example insulin pumps and CGM systems, so the vendors have their offices in the USA, which again means they have their service desks in the USA. (...) diagnostic and service issues are handled, which ultimately leads to some data needing to be sent to the USA anyway.” [Interviewee #3, Sykehuspartner]

Though this was not part of the agreement regarding data storage but rather how data is processed, it is considered a minor issue. Have access to product support and troubleshoot faulty equipment and rectify errors on devices and systems. Sykehuspartner concluded that:

“Assumed that the data sent to the USA is only used for service and troubleshooting. The risk associated is assumed to be low compared to the ability to troubleshoot equipment.” [Interviewee #6, Sykehuspartner]

Sending equipment data to the US there is still some privacy risk related to the matter. But as a part of the manufactures often are based in America there is not much that can be done.

Bigger part of the challenge of data transfer is related to cybersecurity aspects. To follow regulations, vendors need access to logs for effective logging and monitoring. Event detection and logging are critical to detect errors or suspicious activity. Data storage capability is also important for logs, so forensic research can be conducted if an incident occur. Vendor informed:

“As suppliers, we are legally obligated to monitor the medical solutions we deliver. One way we can comply and monitor the secure functionality of our products is by retrieving datasets with logs.” [Interviewee #1, Vendor]

When asked about the laws and regulations, the vendor responded:

“There is EU regulatory laws, EU MDR are regulations for medical devices in Europe. (...) new regulations as Cyber Resiliency and NIS2 on the way also. (...) Companies also have to comply laws and regulations in the USA, example FDA standards for Medical Device Interoperability and their own ISO/IEC standards compliances.” [Interviewee #1, Vendor]

Vendors and manufacturers must follow regulations for post-market surveillance booth from EU and US requirements. Booth from existing EU regulations as MDR and future EU regulations as Cyber Resiliency and NIS2. Understanding that the vendors need to comply to information and cybersecurity laws, they would need certain data from insulin pumps and CGM systems. Seemingly that data sent for post-market surveillance in EU is still somewhat a part original agreement for data storage. Following up on topic vendor stated:

“GDPR does not deny access as arguments can be made for a legitimate use of data. (...) systems are used geographically in Europe, the headquarters are based in USA. A consequence of that some data is sent to the US.” [Interviewee #1, Vendor]

“The data for logs is technical data, and should not have any privacy details, but the data comes from systems that are in use.” [Interviewee # 1, Vendor]

Informing that in some cases data from medical devices are sent to the US after all. Vendor followed up by information the data sent for cybersecurity reasons such as logs of technical data. Therefore, data involved for the post-market surveillance should in theory not include privacy details. Though medical equipment is used in EU, the vendors still have to full fill regulations and standard in the US. Following up on the conversation of the need to send data to the US the vendor said:

“Hospital networks have a tendency being compromised; therefore, many vendors segregate the network and process the data on their own systems.” [Interviewee #1, Vendor]

Combination of practical reasons of working with data on their home soil, there is also cybersecurity aspect by stating segregated from the hospital networks.

The result of this contradiction that vendor will have the need of certain datasets because of practical reasons. Both for be able to deliver product support and troubleshooting, and to follow laws and regulations regarding information security and cybersecurity. Ultimately resulting into some data will be transferred from the EU to USA after all.

This stage showed relevance of contradictions privacy concerns occurring in this stage while insulin pumps and CGM while in use

4.4.4 Stage 4 Use

Fourth stage is after the user have their medical equipment up and running. The factor for identifying this stage was the users talked about use of the equipment after receiving it. The contradiction about third-party applications returns here, as users talks about the topic:

“It is entirely up to me if I want to use more of the functionalities than the standard CGM monitoring. (...) easily connect to an app on my phone for example.” [Interviewee #10, User]

“Mainly I use the standard equipment, it is a small device, screen, that shows my CGM. (...) it is connected to my app too, but I don’t use as much.” [Interviewee #9, User]

As the hospitals also are aware of the applications, in stage they help the users to set up the equipment, from the following statements inform a part of process of happens after the consultation meeting occur in the next stage:

“(...) help to set that up, but we are aware of the extra possibilities they have with the equipment.” [Interviewee #8, Hospital]

This stage turned to be the final finding, as there were no contradictions revealed relevant to any later stages for this research.

4.4.4.1 Third-party Applications

After the hospital and Behandlingshjelpemidler have delivered medical equipment, the topic of third-party applications reoccurs when speaking to users. This contradiction revolves around

the fact that to be able to use third-party applications and its functionality, the users also must agree to the applications Term of Service. Understanding that the extra functionalities are beneficial for daily use, asking about how it can be beneficial users stated:

“While driving the use of CGM applications helps in planning for breaks. I can have my phone show the live monitoring.” [Interviewee #10, User]

“Mostly using the app to help automatically create rapports that show my glucose for a given period of time for my doctor.” [Interviewee #11, User]

“(…) can add my meals in the app, and the app helps me predict my glucose levels, so I can plan ahead, instead of only having live monitoring where I have to rather “react” all the time.” [Interviewee #9, User]

Understanding why this becomes a contradiction lies in the complexity of the Terms of Service, the users must agree to be able access the extra functionality. The contradiction in stage 2 highlights privacy concerns previously expressed by Sykehuspartner. By agreeing to the ToS, medical data is processed outside the healthcare systems and network, raising significant privacy issues.

“(…) extensive info documentation, which leads to no one really reads them.” [Interviewee #8, Hospital]

“When agreeing to the terms, the applications get access to data from the continuous monitoring, and probably other privacy details.” [Interviewee #3, Sykehuspartner]

The Terms of Service agreements have shown to be very long and hard to understand. As Sykehuspartner have expressed privacy concerns of the unknow of the data transfer and storage. Following up if the users have the same concerns they said:

“Really don’t care about it, I know it is a grey area, but prefer using the app anyways.” [Interviewee #9, User]

“I was not aware of how it could be a problem, but I’m not too worried about someone reading my monitoring.” [Interviewee #11, User]

“It is a complicated topic, to be able to use the functionalities in the apps, you have to agree. (…) concerns about the user data. Bringing this to “Datatilsynet” and they would make a case and find cause to impose sanctions, it could result the apps being removed from the Norwegian Appstore, and everyone would lose access to the useful functionality the apps offer.” [Interviewee #10, User]

Users are not obligated to use third-party applications since the standard equipment functions adequately without them. However, the contradiction arises from the fact that these additional functionalities significantly enhance the user experience with the devices. Accessing them requires users to agree to ToS whose consequences they may not fully understand. This contradiction differs from the other contradictions in the earlier stages, as it entirely depends on the user whether they put themselves in this situation. If a user decides that the standard equipment meets their needs sufficiently, they can avoid the contradiction of accepting ToS for extra functionality.

4.4.4.2 Training-data

Contradiction of training-data re occur as from stage 1. Not directly connected to the tension in stage 1, this contradiction of training-data revolves more about the unknown. Building upon the previous contradiction of agreeing to ToS consequently lose control over privacy and medical data. When asked whether data from third-party applications are used as training data, Sykehuspartner stated:

(...) third-party applications are beyond our control, as these applications operate outside our infrastructure. (...) Using this application there is a chance patient data is then used for training. [Interviewee #6, Sykehuspartner]

“(...) issue with the applications are that we lose the control over the data and cannot say for sure what is it used for or not.” [Interviewee #3, Sykehuspartner]

There is no concrete evidence confirming or denying that vendors use Norwegian patient data to improve their equipment. Asking the hospitals about this issue regarding the data processing agreement, they stated:

“The agreements for the applications are between the users and app-creator. (...) We can only adhere to the agreement made between the hospital and patient.” [Interviewee #8, Hospital]

Result of the contradiction that the hospital must accept the uncertainty if Norwegian patient data is used for training purposes or not. The overall lack of control over the data to which applications have access too, create uncertainty if privacy concerns are also valid.

4.5 Summary of Contradictions

Table X have been created to summarise the discovered contradictions. The table is created in four segments representing each stage. Each stage will have the attributes of the number and name for the contradiction, information, stakeholders, result, reasoning, and the source.

Each contradiction is assigned a name, and summarised information about the tension between stakeholders that is presented as “A” and “B”. The outcome is denoted by either “A” or “B” indicating who prevails, with “C” representing cooperation toward a new solution to move forward. Summarised reasoning for the outcome of the contradiction. And a table for who contributed to with information on the topic.

Summary of Contradictions							
1. Acquiring new Equipment							
#	Contradiction	Information	Stakeholder A	Stakeholder B	Result	Reasoning	Source
1.1	Data Storage	Hospital wanted originally to store and process data locally, vendors wanted to store data in the US.	Hospital (Sykehusinnkjøp)	Vendor	C: Store data in EU-cloud services	Due to GDPR & Schrems II compliance to store data in EU.	Vendor, Sykehusinnkjøp, Sykehuspartner, Hospital
1.2	Training-data	Vendors want to use data to improve their products.	Vendor	Hospital	B: Not allowed to use as training data	Hospitals DPA do not agree to use patient data as training data.	Sykehuspartner, Hospital
1.3	Specific Demands	Hospitals requiring too specific functionality or cybersecurity standards.	Hospital (Sykehusinnkjøp)	Vendor	B: Buy provided solutions	Norway as a small client, vendors return of investment will be too low.	Vendor, Sykehusinnkjøp
2. Integration							
#	Contradiction	Information	Stakeholder A	Stakeholder B	Result	Reasoning	Source
2.1	Information Security Details	Information management requires full system documentation	Sykehuspartner	Hospital	B: Deviation in documentation and risk-assessment accepted	Patient treatment always comes first.	Sykehuspartner, Hospital
2.2	Third-party Application	CGM 3-party application for more functionality, lose control over data	Sykehuspartner	Hospital	C: Encourage Hospitals to inform users of privacy risk	Hospitals cannot deny users using 3-party applications but can inform about privacy risk.	Sykehuspartner, Hospital

Table 4. 1: Summary of Contradictions

Summary of Contradictions (Continued)

3. Deployment							
#	Contradiction	Information	Stakeholder A	Stakeholder B	Result	Reasoning	Source
3.1	Device Selection	Users cannot select specific medical equipment; changes are allowed only for medical reasons	Hospital	User	A: User can not choose equipment	Due to the complex procurement process and cost considerations, patients receive suitable and cost-effective equipment.	User, Hospital
3.2	Data Processing and Storage	Though agree upon to store data in EU, there is a need to process data to US for practical reasons	Vendor	Hospital, Sykehuspartner	A: Data and datasets will be used as vendors are needed too	Laws and regulations and for practical reasons, some data need to be sent to the US.	Vendor, Sykehuspartner
4. Use							
#	Contradiction	Information	Stakeholder A	Stakeholder B	Result	Reasoning	Source
4.1	Third-party Application	CGM-system may have the option to use 3-party apps, data is sent outside original network	User	Vendor	B: Users agree to ToS	Users must agree to the Terms of Service to access extra functionality and may not understand the associated privacy risks.	Sykehusinnkjøp, Sykehuspartner, Hospital, User
4.2	Training-data	Users agree to the ToS, there is a possibility that the data may also be used for training purposes.	Hospital	Vendor	C: No control over data used in 3-party apps	There is no evidence whether vendors do or do not use the data for training purposes.	Sykehuspartner, Hospital

Table 4. 2: Summary of Contradictions (Continued)

Chapter 5

Discussion

The goal of the study is to see how the different stakeholders relating to IMDs resolve their contradictions in the Norwegian healthcare. Identifying contradictions and their outcomes can reveal how information security for IMDs is managed in practice. This provides an opportunity to highlight whether current practices are effective or if some should be revised. Comparing the contradictions outcomes to the existing literature can help do give an indication whether it is done by best practice or if there really are any possible alternatives. To be able to discuss how contradictions are solved, the following research questions needed to be answered:

What are the information security contradictions encountered during the implementation stages of Implantable Medical Devices and how are they solved?

5.1 Theoretical implications

Comparing the empirical findings of this research to existing literature highlights how this study contributes to, challenges, or extends current understanding and knowledge. Research on the implementation of IMDs in the Norwegian healthcare system, viewed through the lens of contradiction management, has helped to identify challenges for stakeholder for IMDs that are ongoing in the healthcare sector. Using stage modelling to explain where in the implementation process the contradictions occur, emerge, evolve and resolved across different settings and context within the healthcare system. This new approach has the potential to contribute to a broader theoretical understanding of the implementation process. As such insights can be valuable developing adaptive strategies that can be used for various stages of an implementation of IMDs. Application of stage modelling has also allowed for visualisation of the dynamics of the implementation process, helping to underscore similarities and differences from the existing literature.

The findings demonstrated that different outcomes of the contradictions had varied results of the level for information security. When it came to contradictions and processes revolving technical solutions regarding data storage and data processing, it resulted in high levels of information security. In stage 1 the topic of data storage and training-data, the resolution was to follow cybersecurity regulations and data processing agreements for the Norwegian patients. Same in stage 3, regarding data storage and processing, even though the outcome of contradiction could be seen as unexpected, the result was data transfer to enhance cybersecurity. On the other hand, show where the human element becoming a factor, the level of information security somewhat diminishes. As a result of the contradictions regarding third-party applications users seem to choose an option that potentially led to privacy concerns. Even though the information security concerns for the use of these applications are known. A similar case during stage 2 regarding the contradiction of information security management to establish documentation and a complete risk assessment, the urgent necessity for medical equipment would prevail finish the documentation. The human element here is involved, but more in the factor that need patient treatment will always come first. This indicates the complexity of the environment implantable medical devise interact and engage with.

5.1.1 Laws, Regulations and Standards

The literature showed considerations for cybersecurity laws, regulations and standards. Consensus expressing the need for more effort working on the subject area. This research also would suggest more effort in the subject area, but is also demonstrated operational effectiveness of existing laws, regulations and standards. Part of Williams & Woodward (2015) conclusion was effort regulations and standard would improve and enhance cybersecurity for IMDs. Result of the contradictions where data storage and data processing are involved indicate an enhanced cybersecurity outcome due to laws and regulations. The result of contradiction 1.1 was not a resolution of the stakeholders' original preference, but due to a result of progression of laws and regulations, and the latest Schrems II verdict, resulted the data being stored in EU. Further supporting regulations and standards improved cybersecurity is the practical result of contradiction 3.2. As a consequence of regulations for post-market surveillance forced by authorities and medical equipment organisations need to follow security standards, they needed access to certain datasets. Resulting in IMDs logs being used for monitoring for cybersecurity threats and malfunction equipment, overall enhance the security and safety for the users.

5.1.2 IMDs environment

Standard also being a tool enhance information security management. Contradiction 2.1 is an effect of one stakeholder wish to enforce the need for full documentation and risk assessment to comply with regulatory standards for information security. The result from this contradiction correlates well Camar et al. (2015) finding that despite theoretical security solutions, the practical implementation challenges IMDs a face with will make it challenging. The eventual result of a stalemate of the need of information security documents and the need to use medical equipment, will always favour the need to use the equipment. Patient treatment will always come first, and information security must become second priority. Camar et al. (2015) concluded that effective utilisation and heightened security awareness among users and medical personnel are crucial for achieving success. As the result of contradiction 2.2 regarding privacy concerns to third-party applications, both stakeholders were aware related problems to privacy. Showing that even though patient treatment comes first, do not necessarily mean that cybersecurity of any means is neglected by the Norwegian healthcare personnel. Literature commonly separate healthcare and cybersecurity as separate domains, the cybersecurity awareness expressed from the health personnel might indicate the domains being more integrated than previously anticipated.

5.1.3 Third-party Application

Another key finding was the contradictions surrounding the use of third-party applications for CMG systems. Unlike regulations concerning data processing and storage, Britton & Britton-Colonnese's (2017) survey on applications and regulations revealed a grey area regarding whether certain health and medical applications are required to comply with regulations. In general, patients and users have the right to control their own personal data. However, the lack of laws and regulations regarding application raises privacy concerns. In general, hospitals cannot impose restrictions on patients' use of applications, but lack of legal frameworks and regulations also makes it harder to adequately educate about the privacy risk revolving the use of

applications. Randine et al. (2023) research aligns with the finding that there is necessarily no need to use applications, as the standard equipment from the hospitals is enough to treat diabetes. The findings that users perceive the applications beneficial are in parallel from the literature. The conclusion from Randine et al. (2023) is the complexity of the Terms of Use hinders users from fully understanding and comprehending what they are accepting and agreeing to, due perceiving the application as beneficial. Consistent with the literature the same dilemma has been distressed in the findings in contradiction 4.1.

5.1.4 Users' needs

Initially not seeing contradiction 3.1 as a particularly interesting, one speculated reason for users resorting to third-party applications could be dissatisfaction with hospital-provided device functionality. The research did not delve deeper into whether standard CGM devices generally lack sufficient functionality, prompting users to turn to third-party applications. Alternatively, allowing users to select fitting equipment might dissuade them from using third-party applications, potentially minimizing privacy concerns. Addressing the importance of understanding the environments in which IMDs are used is crucial, as emphasized by William & Woodward (2015), who advocate for collaboration among medical physicists, IT professionals and manufacturers. Adding patients and users to the collaboration list could be equally important as they are the end users of these devices. Underscoring this, the findings there is pattern that contradictions involved users the result are not the optimal solution for cybersecurity. While existing literature has a more technical approach of cybersecurity for IMDs design and development. It can be argued that from an overall cybersecurity perspective understanding the users and patients use of devices are important. Camara et al. (2015) highlight the practical obstacles implementing of IMDs necessitates increased security awareness among users and medical personnel. This underscores the importance of integrating such understanding from the very start of the IMDs design and development processes.

5.2 Practical implications

Practical implications will focus on how the research findings can be applied to improve information security practises for IMDs. This research has investigated the stakeholders' dynamics during the implementation of IMDs and can be used as guidance to anticipate and manage other contradictions in the healthcare.

Using stage modelling is a tool to help to visualise the evolution of resolution of contradictions during the implementation. The approach of stage modelling can be used as framework for developing adaptive strategies tailored to different stages implementation IMDs and other relevant medical equipment. The lens of contradiction management can also help to indent challenges that need to be solved, but also understand the dynamic between and need for stakeholders. Which is important in a interconnected environment like the health sector. Combining these practices can guide and manage cybersecurity challenges, from both existing and future endeavours.

5.2.1 Cooperation

The intricate environment in which IMDs operate involves numerous stakeholders with diverse roles, all sharing a commitment to information security and cybersecurity. This shared mission makes collaboration challenging yet essential. One key factor for success is enhanced cooperation among all stakeholders. IT and cybersecurity professionals excel in their domain, while healthcare professionals bring expertise in theirs. It is crucial to integrate these domains to effectively create, implement, and utilise IMDs from both cybersecurity and safety perspectives. Additionally, considering the importance of patients and users within this intricate environment is paramount. Combining expertise with a user-centric approach can prove beneficial across various scenarios, from initial cybersecurity design and development to the practical use of these devices. Cooperation, where each stakeholder addresses their needs and goals, is vital for achieving optimal outcomes. While satisfying all stakeholders completely may remain a challenge, continuous improvements in today's cybersecurity landscape should be achievable.

5.2.2 Cybersecurity awareness

The landscape for use of IMDs today there are cybersecurity and privacy concerns. While future research and development efforts may eventually mitigate these concerns, they remain prevalent in current situations. One effective approach to addressing these issues is to promote cybersecurity awareness for IMDs. Cybersecurity awareness plays a critical role at every stage of IMDs. It starts with vendors ensuring the creation of secure and safe products. Procurement teams must be vigilant about cybersecurity challenges when selecting equipment. IT and cybersecurity professionals need to make informed decisions to safeguard these devices. Additionally, medical professionals must be trained and informed in cybersecurity protocols and awareness for using medical equipment to enhance cybersecurity. Equally important is raising awareness among patients and users to empower them to take educated decisions and contribute to the cybersecurity efforts.

5.2.3 Regulations and standards

Following information security and cybersecurity regulations and standards has proven effective in enhancing overall information security and cybersecurity in this research. However, it is evident that there remains a gap between current regulations and the rapidly medical equipment landscape seen from the example of CGM applications. Despite this, adherence to existing regulations and standards continues to have a positive impact. Future laws, regulations, and standards are advancing progressively to further enhance cybersecurity for medical equipment in general. Therefore, everyone involved in designing, developing, and implementing IMDs in healthcare should strive to comply with cybersecurity regulations and standards. While practical challenges may arise in the healthcare sector, it is generally advisable to adhere as closely as possible to regulations and standards to strengthen cybersecurity measures. Building upon the cooperation, it is important for healthcare professionals, patients, and users to voice their perspectives. This ensures that upcoming regulations are not solely dictated by cybersecurity experts and lawyers, potentially making the regulations impractical and challenging to implement and use in healthcare settings

5.3 Future Work

This research has given a better understanding of the implementation of IMDs. The research has given a surface-level view of the implementation. Future research can investigate the entire implementation more deeply. Examine each identified step closely. For example, within the umbrella concept of hospitals, there are potentially several stakeholders who can contribute deeper perspectives with more precise and insightful understanding. At both ends of the stages also, encompassing procurement and the process spanning from tendering to contract signing, numerous critical stages pertain to information security. Likewise, a closer examination of the interaction between healthcare professionals and patients, and patients use of medical equipment over time has the potential to yield valuable insights.

Using the lens of contradiction management and stage model could be interesting from the start to finished of the production of IMDs. Potentially giving valuable insight and understand of choices taken during the design and development process. Compare the choices taken at early stage of the lifecycle of IMDs and see how the after-health personnel and users at later stages.

From the literature there were some identified challenges relating to applications and regulations. In the findings there were also some challenges revolving information security management practices and privacy concerns relating to applications. There could be interesting to follow the progress of the coming work from authorities on laws regulations and standards. Investigate how they address relevant cybersecurity issues for medical equipment and IMDs.

This research approach has helped to understand stakeholders and see how some information security and cybersecurity work in practice. Takings from this research, endorse researching the topic of IMDs and cybersecurity with new approaches. To potentially find and highlight new discoveries and observations or even confirming existing research. So the field of IMDs can be more widely covered to enhance the cybersecurity and safety so patients and users can trust and thrive with their implantable medical devices.

5.4 Limitations

The limitation section is to reflect and discuss the shortcoming and constraints of the research. In this research, the scope was limited to the healthcare sector of south-east of Norway. This may restrict the applicability and transferability for other nations or healthcare organisations. Potential constraint imposed is time have restricted the depth of exploration, that continues work on the research could potentially discovers more relevant for the literature review and contradictions during implementations of IMDs in the Norwegian healthcare.

Additionally, there are constraints on number of interviewees and diversity from various organisational background. The healthcare sector has proven to be difficult to get in touch and schedule an interview. Honest feedback from the healthcare sector there is limited time available and the endless responsibilities and tasks to be done. Vendors for medical equipment have also been proven hard to get in touch with, as most inquiries have declined and ignored. To countermeasure this limitation it has been important that all discovered contradictions have at least two sources, so a contradiction do not only present one organisations perspective only.

Using the research approach of contradiction management, process theory and stage modelling itself can be a limitation. As these theories and model may be complex and requiring a significant amount of time and effort to fully understand and apply correctly. Also using qualitative methods, basing on generating hypotheses and articulating an understanding from data by the researchers understanding. All informants have had their chance to verify finding to reduce the wrong assumptions and give robustness to the outcome.

Chapter 6

Conclusion

This research has investigated information security contradictions that occur during the implementation of implantable medical devices in the healthcare. The research approach was conducted through the lens of contradiction management and supported by process theory and stage modelling. The goal for this approach was look at IMDs from a new perspective and potentially lead to new insights and confirming or contrary existing literature.

The research identified relevant stakeholders for IMDs and discovered several contradictions throughout the implementation process. Discovered contradictions were placed in the suitable stages that was identified during the implementation process. The main topics for these contradictions were data storage and processing, information security management, and the use of CGM applications. Some contradiction topics reoccurred in different stages, albeit with some variations. The complexity of the environment in which IMDs are used affected the nature of these contradictions. Contradictions in an environment focused on solving IT problems had somewhat higher levels of cybersecurity compared to those solved in healthcare, patient, and end-user environments.

These findings contribute to the literature of IMDs for several aspects. First confirming work on laws, regulations and standards influence how IMDs are implemented in the healthcare. Second the findings highlight the complexity of combining information security and cybersecurity in a healthcare, patient and ed-users setting. Last confirming the need for continues research and work to enhances the cybersecurity and safety for IMDs.

This thesis also confirms that by exploring and researching using different approaches than before in the domain of IMDs and the environments they operate in, it can potentially provide insight from new perspectives. Ultimately, this may contribute to enhanced understanding from all parties, leading to a desired outcome where overall cybersecurity and safety for IMDs improve.

In conclusion, this research underscores the ongoing necessity and focus for information security and cybersecurity for IMDs. To design, develop, implement, and utilise IMDs in a secure and safe manner, understanding the devices' complex environments and lifecycles is crucial. Continuous research and effort in a rapidly changing and evolving environment aim to enhance cybersecurity and safety, fostering trust and enabling users to thrive with their IMDs.

Bibliography

- Alexander, B., Haseen, S. & Baranchuk, A. (2019). Are implanted electronic devices hackable? *Trend in Cardiovascular Medicine*, Volume 29. <https://doi.org/10.1016/j.tcm.2018.11.011>
- Balas, V. & Pal, S. (2020). *Healthcare Paradigms in the Internet of Things Ecosystem*. Academic Press.
- Britton KE. & Britton-Colonnese JD. (2017). Privacy and Security Issues Surrounding the Protection of Data Generated by Continuous Glucose Monitors. *Journal of Diabetes Science and Technology*, Volume 11. <https://doi.org/10.1177/1932296816681585>
- Camara, C. Peris-Lopez, P. & Tapiador, J. (2015). Security and privacy issues in implantable medical devices: A comprehensive survey. *Journal of Biomedical Informatics*, Volume 55. <https://doi.org/10.1016/j.jbi.2015.04.007>
- Domingo-Lopez, D., Lattanzi, G., Schreiber, L., Wallace, E., Wylie, R., O'Sullivan, J., Dolan, E. & Duffy, G. (2022). Medical devices, smart drug delivery, wearables, and technology for the treatment of Diabetes Mellitus. *Advanced Drug Delivery Reviews*, Volume 185. <https://doi.org/10.1016/j.addr.2022.114280>
- Hargrave, T. J. & Van de Ven, A. H. (2016). Integrating Dialectical and Paradox Perspectives on Managing Contradictions in Organizations. *European Group for Organizational Studies*. Volume 38. <https://doi.org/10.1177/0170840616640843>
- Hassija, V., Chamola, V., Bajpai, B. C., Naren & Zeadally, S. (2021). Security issues in implantable medical devices: Fact or fiction? *Sustainable Cities and Society*, Volume 66. <https://doi.org/10.1016/j.scs.2020.102552>
- Helse Sør-Øst RHF. (2024, 03.05). Om oss – Regionalt helseforetak som sørger for spesialhelsetjenestetilbud. <https://www.helse-sorost.no/om-oss/>
- Hennink, M., Hutter, I., Bailey, A. (2020). *Qualitative Research Methods*. Sage.
- Joung, Y-H. (2013). Development of Implantable Medical Devices: From an Engineering Perspective. *International Neurology Journal*, Volume 17. <https://doi.org/10.5213/inj.2013.17.3.98>
- King, W. & Teo, T. (1997). Integration Between Business Planning and Information Systems Planning: Validating a Stage Hypothesis. *Decision Sciences*, Volume 28. <https://doi.org/10.1111/j.1540-5915.1997.tb01312.x>
- Klonoff, D. & Han, J. (2019). The First Recall of a Diabetes Device Because of Cybersecurity Risks. *Journal of Diabetes Science and Technology*, Volume 13. <https://doi.org/10.1177/1932296819865655>
- Kropff, J., Chaudhary, P., Neupane, S., Barnard, K., Bain, S., Kapitza, C., Forst, T., Link, M., Dehennis, A. & DeVries, J. (2017). Accuracy and Longevity of an Implantable Continuous Glucose Sensor in the PRECISE Study: A 180-Day, Prospective, Multicenter, Pivotal Trial. *Emerging Technologies and therapeutics*, Volume 40. <https://doi.org/10.2337/dc16-1525>

- Kwarteng, E. & Cebe, M. (2022). A survey on security issues in modern Implantable Devices: Solutions and future issues. *Smart Health*, Volume 25.
<https://doi.org/10.1016/j.smhl.2022.100295>
- Langley, A., Smallman, C., Tsoukas, H., & Van De Ven, A. (2013). Process Studies of Change in Organization and Management: Unveiling Temporality, Activity, and Flow. *Academy of Management Journal*, Volume 56. <https://doi.org/10.5465/amj.2013.4001>
- Miles, M., Huberman, M. & Saldana, J. (2013). *Qualitative Data Analysis* (3 edition). SAGE Publications Inc.
- Myers, M. D. & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and Organization*. Volume 17.
<https://doi.org/10.1016/j.infoandorg.2006.11.001>
- Nasjonal Nettverksgruppe for Behandlingshjelpemidler. (2024). Om Nasjonal Nettverksgruppe for Behandlingshjelpemidler. <https://behandlingshjelpemidler.no/om-nnb/>
- Niemimaa, M., & Niemimaa, E. (2019). Abductive innovations in information security policy development: an ethnographic study. *European Journal of Information Systems*, Volume 28.
<https://doi.org/10.1080/0960085X.2019.1624141>
- Pycroft, L. & Aziz, T. (2018). Security of implantable medical devices with wireless connections: *The dangers of cyber-attacks*. *Expert Review of Medical Devices*, Volume 15.
<https://doi.org/10.1080/17434440.2018.1483235>
- Randine P, Pocs M, Cooper JG., Tsolovos D., Muzny, M., Besters, R. & Årsand, E. (2023). Privacy Concerns Related to Data Sharing for European Diabetes Devices. *Journal of Diabetes Science and Technology*. <https://doi.org/10.1177/19322968231210548>
- Recker, J. (2021). *Scientific Research in Information Systems A Beginner's Guide*. Second Edition. Springer.
- Regjeringen. (2023, 16.01). Grunnstrukturen i helsetjenesten.
<https://www.regjeringen.no/no/tema/helse-og-omsorg/sykehus/vurderes/grunnstrukturen-i-helsetjenesten/id227440/>
- Siddiqi, M., Seepers, R. M., Hamad, M. Prevelakis, V. & Strydis, C. (2018). Attack-tree-based Threat Modeling of Medical Implants. *Kalpa Publications in Computing*, Volume 7, 32-49.
<https://doi.org/10.29007/8gxx>
- Soliman, W. & Ojalainen, A. (2023). *Conflict Resolution in an ISO/IEC 27001 Standard Implementation: A Contradiction Management Perspective*. Hawaii International Conference on System Sciences, Hawaii. <https://hdl.handle.net/10125/103223>
- Solli-Sæther, H. & Gottschalk, P. (2010). The Modeling Process for Stage Models. *Journal of Organizational Computing and Electronic Commerce*, Volume 20.
<https://doi.org/10.1080/10919392.2010.494535>
- Steen, T. (2020). Kvalitetskontroll av implanterte hjertestartere. *Tidsskriftet*, Volume 140.
<https://doi.org/10.4045/tidsskr.20.0674>

- Sykehusapotekene. (2023, 24.04). Om oss – Vi er sykehusenes og pasientenes kompetansesenter for legemidler. <https://www.sykehusapotekene.no/om-oss/>
- Sykehusinnkjøp. (2024, 19.02). Om oss – Sjukehusinnkjøp HF skal utøve ei spesialisert og profesjonell innkjøpsteneste for spesialisthelsetenesta. <https://www.sykehusinnkjop.no/om-oss/>
- Sykehuspartner. (2024, 17.04). Om oss – Gode og likeverdige helsetjenester til alle som trenger det, når de trenger det. <https://www.sykehuspartner.no/om-oss/>
- Webster, Jane & Watson, Richard, T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*. Vol. 26, NO. 2. <https://www.jstor.org/stable/4132319>
- Werner C. M., Baxter L. A. (1994). Temporal qualities of relationships: Organismic, transactional, and dialectical views. In Knapp M., Miller G. (Eds.), *Handbook of interpersonal communication*. Second edition. Thousand Oaks, CA: SAGE Publications
- Williams, P. A., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. *Medical Devices: Evidence and Research*, Volume 8, 305–316. <https://doi.org/10.2147/MDER.S50048>
- Wilner, A., Luce, H., Ouellet, E., Williams, O. & Costa, N. (2022). From public health to cyber hygiene: Cybersecurity and Canada’s healthcare sector. *International Journal*, Volume 74. <https://doi.org/10.1177/00207020211067946>
- Xiao, Yu & Watson, Maria. (2019). Guidance on Conducting a Systematic Literature Review. *Journal of Planning Education and Research*. Volume 39, Issue 1. <https://doi.org/10.1177/0739456X1772397>

Appendix A Interview guide

Intervjuemal - Motsetninger mellom interessenter involvert i livssyklusen til pasient nært utstyr

Søkelys på informasjonssikkerhet og personvern.

Semistrukturert – fokus og åpenhet for dialog.

Dette er kun eksempel mal, da intervjuobjekter kommer fra forskjellige bakgrunn.

Bakgrunnsinformasjon:

1. Hva er din stilling og hvem jobber du for?
2. Hva er din jobb i helsesektoren eller relatert til helsesektoren?

Kjennskap til implementeringsprosessen:

3. Hva er dine erfaringer med prosessen for implementering av pasientnært klinisk utstyr?
 - a. Finnes det noen utfordringer?
 - i. Hvordan blir løst?
 - ii. Kan det bli løst på andre måter?
 - b. Andre innspill?
4. Hvem er aktører i en slik prosess?

Informasjonssikkerhet og personvern:

5. Hva er din kjennskap til datasikkerhet og personvern relater til pasientnært klinisk utstyr?
6. Er det noen utfordringer relatert til datasikkerhet og personvern?
 - a. Hvordan blir det løst/ikke løst?
7. Er det noe praktiske utfordringer?
 - a. Hva er eventuelt konsekvensene?

Komplikasjoner med implementering relatert til informasjonssikkerhet og personvern:

8. Kjennskap til utfordringer relater til implementering relatert til informasjonssikkerhet og personvern?
 - a. På pasientnært klinisk utstyr?
9. Hvordan blir dette løst?
 - a. Kan det løses på andre måter?

Komplikasjoner med bruk relatert til informasjonssikkerhet og personvern:

10. Kjennskap til utfordringer relater til bruk relatert til informasjonssikkerhet og personvern?
 - a. På pasientnært klinisk utstyr?
 - b. På behandlingen av data relatert til med pasientnært klinisk utstyr?
11. Hvordan blir dette løst?
 - a. Kan det løses på andre måter?

Ytterligere bidrag:

12. Andre ting som du ønsker å legge til?

Appendix B Consent form

Vil du delta i forskningsprosjektet «Motsetninger mellom interessenter involvert i livssyklusen til pasientnært utstyr»?

Formålet med prosjektet

Dette er et spørsmål til deg om du vil delta i et forskningsprosjekt hvor formålet er å kartlegge ulike motsetninger mellom interessenter for pasientnært klinisk utstyr, med fokus på insulinpumper, kontinuerlig glukose måling, og pacemaker.

- Snakke med ulike aktører fra anskaffelse til bruk
- Oppdage og legge frem motsetninger i ulike faser med pasientnært klinisk utstyr
- Forstå ulike parter og hvordan en kommer frem til felles løsninger

Hvorfor får du spørsmål om å delta?

Du får denne forespørselen fordi:

1. Du er blitt foreslått som en ressursperson på temaet gjennom nettverket i Sykehuspartner.
2. Du er blitt foreslått som en ressursperson gjennom samtale med andre i helsesektoren.

Hvem er ansvarlig for forskningsprosjektet?

Universitet i Agder med Steffen Tendvall Abrahamsen som student er ansvarlig for personopplysningene og data som behandles i prosjektet.

Student: Steffen Abrahamsen, steffenta@student.uia.no

Veileder: Wael Soliman, wael.soliman@uia.no

Personvernombud UiA: Trond Hauso, personvernombud@uia.no

Det er frivillig å delta

Det er frivillig å delta i prosjektet, ingen ting blir gjort uten ditt samtykke. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg. Utvalget har rett til å klage til Datatilsynet om eventuelle overtredelser.

Hva innebærer det for deg å delta?

- Det vil være en sesjon med intervju som varer i fra 10-30 minutter. Det er mulig å motta spørsmålene på forhånd om ønskelig før en takker «ja» til å delta.
- Etter endt intervju ferdigstiller jeg informasjonen fremhevet i intervjuet. Ferdigstiller dette slik at du får en mulighet til å se over mine funn. Dette gir deg muligheten til å korrigere, legge til eller fjerne informasjon.
- Personopplysninger behandlet under innsamling vil være:
 - Navn og
 - Epostadresse
 - Dette brukes kun til kontaktinformasjon.
 - Arbeidstittel
 - Bedriftsnavn
 - Dette brukes i henvisning i oppgaven om avtalt.
 - Helseforetak vil kun presenteres som «helseforetak», og ikke mer spesifikt.
 - Leverandør av medisinsk utstyr vil kun bli presentert som «leverandør», og ikke mer spesifikt.

- Ønsker en å delta og være informant, vil kun din tittel i bedriften og bedriften du presenterer.
- Etter innlevert oppgave vil dine personopplysninger bli slettet. Informasjon som er klart godkjent, vil bli brukt i oppgaven.
- Du kan når som helst be om innsyn, kopi, rette feil, eller be om å slette dine opplysninger.
- Opplysninger og data fra å intervju vil bli notert fysisk eller digitalt. Dette vil bli lagret på sikker Sykehuspartner eller personlig hvelv på OneDrive hvor kun Steffen Abrahamsen har tilgang.

Jeg har mottatt og forstått informasjon om prosjektet, og har fått anledning til å stille spørsmål. Jeg samtykker til:

- å delta i intervju
- at mine personopplysninger lagres til prosjektslutt, 7 juni 2024.

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet

Hvis du har spørsmål knyttet til Sikts vurdering av prosjektet, kan du ta kontakt på e-post: personverntjenester@sikt.no, eller på telefon: 73 98 40 40.