Kristiania
University
College

Master of Information Systems:
Digital Business systems

IoT for Diabetics:
Exploring IoT Adoption Issues

Signe Marie Cleveland
Student Number: 703710

A report submitted in partial fulfillment of the requirement for
the degree of Master of Information Systems: Digital Business systems

Kristiania University College
Prinsens Gate 7-9
0152 Oslo
Norway

Abstract

An increasing problem worldwide is the number of people living with and dying of critical, chronic diseases. One of these diseases is type 1 diabetes, which, as of today, is uncurable yet treatable through careful and precise monitoring. Using the Internet of Things (IoT) is one of the most efficient ways to monitor diabetes and is also said to improve the life-quality of people with diabetes. However, the great potential of IoT in diabetes treatment is followed by various challenged factors regarding privacy and security. Cyberattacks can affect not only the individual patient but everyone connected to the IT infrastructure of the hacked device. Existing reports show cyberattacks against the Norwegian healthcare sector have increased by 72% over the last year, resulting in about 450 attacks each week. Still, diabetic patients tend to trust their devices to be safe and are willing to take the risk as they consider their medical data as not interesting to cybercriminals. Healthcare personnel's lack of knowledge about information security and privacy best practice is reported to be an entry point for cybercriminals to gain access to critical IT systems. This study aimed to investigate the relationship between the potentially improved life-quality from using diabetes IoT and the challenges regarding privacy and cyberthreats, including the perspective of three different Norwegian stakeholder groups: diabetic patients (type 1), healthcare personnel working with diabetes patients, and industry representatives within healthcare and security. Findings suggest that neither patients nor healthcare personnel is concerned about patient privacy or threats against diabetes IoT, despite the increased cyberthreats in the healthcare sector. It further indicates a pressing matter for a discussion about data ownership generated by IoT and a revision of privacy regulations that make it easier for all Norwegian healthcare regions to interpret, comply, and act upon equally, to utilize the technology available and ensure diabetes patients all over the country have the same opportunities when it comes to patient care.

Keywords: Privacy, Cybersecurity, IoT, Internet of Things, e-health, Healthcare, Diabetes

Acknowledgments

I am forever grateful to several people who have generously supported me through not only the process of completing this thesis, but my master's degree all together.

Firstly, I would like to thank my supervisor, Moutaz Haddara, for valuable and constructive guidance, reviews, and instructions. I have genuinely appreciated your lectures, our discussions, and your support through these years, which has introduced me to a passion for healthcare technology and cybersecurity I didn't know existed.

I would also like to thank my friends, boyfriend, and family for the encouragement during this period. Kakerådet and Kef, thank you for the enormous support throughout my academic years, for always seeing the light when all I see is dark, proofreading my exams, and discussing ideas even though it has been beyond your field of interest. Espen, thank you for being such an emotional support and keeping me sane when I'm losing it these last months, I don't even think you're aware of your impact. Dad, grandma and grandpa, mom, thank you for always believing in me, having my back, and cheering me on. I love you so much.

Finally, my deepest gratitude goes to the participants in the study. It would not have been possible without the patients, nurses, doctors, and industry representatives, who have been so kind to participate despite their busy schedules. You have all provided me with valuable, helpful, and interesting information and potential sources of information.

I certify that the work presented in the thesis is my own unless referenced.

Signature: Signe Marie Overland

Date: 25.05.2022

Total number of words: 21656

Table of Contents

List of figures

List of tables

1. Introduction

The number of people being diagnosed with and dying of chronic diseases, such as diabetes, is increasing worldwide and is expected to surge in the years to come. World Healthcare Organization estimates that 1.5 million deaths in 2019 were directly caused by diabetes (WHO 2021). Recent numbers estimate that 345 000 people in Norway live with diabetes (FHI 2020). Type 1 diabetes is a life-threatening disease that occurs when the body cannot produce the hormone insulin, resulting in the need for daily administration of insulin injections to regulate glucose levels. Other complications include developing other life-threatening diseases such as heart attacks and kidney failure (Diabetesforbundet 2022; Harvard Medical School 2022; WHO 2021). 2022 marks 100 years of successful insulin treatments. On January 23rd, 1922, a 14-year-old boy named Leonard Thompson, who had been dying for over a month, received the first successful insulin injection, which lowered his glucose levels by 80% in 24 hours. This was described as a medical revolution; the world received a treatment for diabetes that would give people who earlier would have died a chance to live longer lives (Hernæs 2022). Despite the discovery of insulin and the medical evolution over the last 100 years, there is still no cure for type 1 diabetes. Glucose levels must be carefully monitored to uphold the patient's health and life-quality. If unmonitored and not treated, diabetes is a deadly disease (Gómez, Oviedo, and Zhuma 2016). The most challenging part of living with type 1 diabetes is that the body requires insulin day and night, and just the precise amount to avoid both high (hyperglycemia) and low (hypoglycemia) glucose levels (Diabetesforbundet 2021; NHI 2020; 2021).

The increased use of Internet of Things (IoT) technology has transformed and revolutionized several sectors worldwide and impacted our modern-day lives. Through sensors and actuators that blend seamlessly into different environments, IoT makes it possible to measure, infer, process, and analyze data and share the information across various platforms for analysis. One sector that has adopted the possibilities and opportunities promised by IoT technology is the healthcare sector (Cleveland and Haddara 2021; Gubbi et al. 2013; Islam et al. 2015). IoT devices for diabetics have been developed to simplify insulin treatment and glucose monitoring. This technology includes wearable sensors and insulin pumps for continuous glucose level monitoring and timely insulin injections (Diabetesforbundet 2021; Rodbard 2016). Research states that these personal medical devices improve short- and long-term glucose levels, make everyday life easier, and improve diabetics' life-quality (Cleveland and Haddara 2021; Longva and Haddara 2019; Diabetesforbundet 2021). The future for diabetes treatment is digital and immediate, as multiple versions of closed loop systems generating real-time data from CGMs and delivering minute-by-minute insulin injection changes is emerging and is said to enhance diabetes treatment even further (Klonoff, Kerr, and Kleidermacher 2017).

However, the increasing digitalization and explosive advancement and adaption of IoT in the healthcare sector, consisting of many components and functionalities, calls for a rapidly growing issue worldwide: a variety of potential cybersecurity threats (Kintzlinger and Nissim 2019; Patil and Seshadri 2014; Rehman, Naz, and Razzak 2021). The cyberthreat level in Norway is increasing, causing sufficient information and privacy security to simultaneously become an important part of the healthcare institutions' responsibilities. Cyberattacks targeting the healthcare sector can cause patient trauma, e.g., by compromising and leaking patients' medical information, modifying data, or disabling healthcare IT systems (Nasjonal Sikkerhetsmyndighet 2022; Riksrevisjonen 2020). Few Norwegian institutions and organizations are prepared for cyberthreats. In 2018, Helse Sør-Øst was exposed for an extensive, successful cyberattack, followed by an attack against Sykehuset Innlandet in 2020. Simulated cyberattacks against the four healthcare regions in Norway performed by The Office of the Auditor General revealed that their IT infrastructures are incredibly vulnerable (Bruvoll, Thuv, and Enemo 2020; Riksrevisjonen 2020).

Previous research has to some extent investigated how the use of IoT in diabetes treatment impacts the life-quality of patients (e.g., Cleveland and Haddara 2021; Longva and Haddara 2019), and there are several studies related to cybersecurity threats and privacy issues in the healthcare sector (e.g., Abdollahi, Moghaddam, and Parvar 2019; Alaba et al. 2017; Britton and Britton-Colonnese 2017). To the author's knowledge, there is still a lack of research investigating how patients and healthcare personnel view the potentially improved life-quality of using IoT in the context of cyberthreats, privacy, and security and how the industry perceives this dilemma. This thesis seeks to follow the recommendation from previous research and investigate the relationship, including the perspective of three different Norwegian stakeholder groups: diabetic patients (type 1), healthcare personnel working with diabetes patients, and industry representatives within healthcare and security (Cleveland and Haddara 2021). The three research questions that helped address this problem were formulated as follows:

RQ1) How does diabetic patients experience their life-quality after changing from manual equipment to IoT-based equipment?

RQ2) How does healthcare personnel (working with diabetic patients) experience patients' life-quality after changing from manual equipment to IoT-based equipment?

RQ3) What are the stakeholders' perspective on privacy and security related issues in using IoT for treating diabetes?

The remainder of this thesis is structured as follows: A thorough literature review is presented in chapter 2. Chapter 3 presents the research strategy and data collection methods adopted for this study. The ethical consideration for conducting research is included in this chapter. Chapter 4 presents the findings from the interviews in a within-case analysis, followed by a discussion of the findings in chapter 5. Lastly, chapter 6 present this study's conclusion, and presents its implications for research and practice, limitations, and suggestions for future research.

2. Literature Review

2.1 Internet of Things in healthcare

Internet of Things (IoT) refers to physical objects (*things*) connected to the internet by outfitting them with sensors and actuators and is a rapidly growing trend within information systems (Perera et al. 2014). IoT provides a universal connection of things, systems, services, and people to collect all sorts of data and communicate directly with each other, other systems, and humans. They communicate through wireless sensor networks (WSN) by gathering data and delivering them to authorized cloud-based resources to be extracted and interpreted (Alaba et al. 2017). Ultimately, the goal of IoT is to enhance the world for human beings, as it enables more data sources which contribute to more educated and richer ground for decision making and is able to act on it without explicit commands (Perera et al. 2014; Saltzstein 2020). By 2025, it is expected that IoT devices will reach over 25 billion (Alaba et al. 2017; Barati and Rana 2020). The term "Internet of Things" was first coined in 1999 in the context of supply chain management but has been adjusted over the last decades and now covers a wide range of applications in several sectors. One of the most attractive application areas for the IoT is the healthcare sector (Gubbi et al. 2013; Islam et al. 2015).

With the growing population of elderly and patients with chronic diseases, causing the cost of health maintenance to increase, there is a need for medical data to be handled in real-time to prevent the disease from getting worse and patients from developing other conditions or dying (Abdollahi, Moghaddam, and Parvar 2019; Alaba et al. 2017; Islam et al. 2015; Shahid et al. 2022). This can be done by integrating IoT, which has proven to be especially beneficial for patients with chronic diseases, such as diabetes (Bhatt and Bhatt 2017). The increased use and potential of IoT for connecting sensors and medical devices and providing real-time patient monitoring without interfering in the patient’s daily life are some of the driving factors of its adoption in the healthcare sector. It has transformed patient care with significant improvements and, promises the power of early detection, prevention, and helps to improve life-quality, to reduce costs (Abdollahi, Moghaddam, and Parvar 2019; Gómez, Oviedo, and Zhuma 2016; Islam et al. 2015; Kintzlinger and Nissim 2019; Patil and Seshadri 2014; Rehman, Naz, and Razzak 2021). In combination with artificial intelligence (AI), wearables and other IoT devices in healthcare are becoming more intelligent and faster in providing information to assist healthcare personnel and are expected to be converted from data collection points to more ingenious devices that can interact in a meaningful manner with the data. Examples of such IoT devices are systems for monitoring glucose levels and pumps injecting insulin for diabetes patients that continuously capture data and transfer it to the cloud to be analyzed and perform an action based on the analysis (Chouffani 2020; Gómez, Oviedo, and Zhuma 2016; Longva and Haddara 2019).

2.2 Patient monitoring

Wearable technology is essential within the healthcare sector. With Wireless Body Area Network (WBAN) technologies, devices consisting of sensors and actuators, healthcare personnel can monitor patient's vital parameters from anywhere at any time and provide the correct medical care at the right time, which can improve the quality of patient care and is critical for some patients (Abdollahi, Moghaddam, and Parvar 2019; Chouffani 2020; Patil and Seshadri 2014; Saltzstein 2020). By monitoring patients’ health and vital systems, wearable technology aims to improve patients' quality of life. Previous research has proven that the use of IoT in diabetes treatment improves diabetic patients’ life-quality (Cleveland and Haddara 2021; Diabetesforbundet 2021; Longva and Haddara 2019; Saltzstein 2020).

Through the years, these sensors and actuators have become cheaper and smaller in size, yet more powerful, and have helped overcome challenges within the healthcare sector when used for patient monitoring purposes (Cleveland and Haddara 2021; Gómez, Oviedo, and Zhuma 2016). These sensor networks consist of one or more sensing nodes that, in a multi-hop approach, communicate with each other. Its three-layer architecture comprises various wearable sensors, which is one of the most recommended frameworks for remote health monitoring. The collected data from these sensors are usually transmitted through a Bluetooth connection to a gateway server, which turns the data into a measurement and observation file that is stored remotely (usually on a cloud-based server) for later analysis. Healthcare personnel can access these files through an online service application (Cleveland and Haddara 2021).

The number of people using IoT devices for medical purposes increases each year (Kintzlinger and Nissim 2019). As many as 80% of consumers are comfortable and willing to use wearable technology that generates medical data and monitors their health 24/7. This trend is expected to continue to grow in the years to come (Lerman 2020). It is predicted that the wearable technology market value will increase by 165%, to $74 billion USD, in the years 2019 to 2025 (Chouffani 2020).

2.2.1 Insulin pumps

Insulin pumps are considered the most efficient therapy for controlling type 1 diabetes and are recommended for all patients with type 1 diabetes by the Norwegian health government. They consist of a minicomputer that infuses insulin into the patient's body through a tube. The pump can either be directly attached to the patient's body, if wireless, or to the patient's belt or stored in a pocket, if wired. It must be replaced or refilled every few days. Insulin pump manufacturers like Medtronic, Tandem, and Omnipod offer pumps that employ IoT-technologies, where the pump is either monitored and controlled directly on the pump itself, through a personal medical device (PMD), an app on smartphones, or by *closed loop* technology in combination with a CGM. Some insulin pumps are compatible with CGMs, meaning the CGM's measurements can be transferred directly to and be read on the insulin pump (Cleveland and Haddara 2021; Diabetesforbundet 2021). Apps for insulin pumps have traditionally been limited to monitoring rather than control of the device in an attempt to minimize cyber risks, however, there is a rising demand among patients for controlling the pumps with their phone to avoid carrying additional devices around (Ahn and Stahl 2019; Klonoff, Kerr, and Kleidermacher 2017). Currently, no insulin pumps can be controlled by an app in Norway, but Tandem has released an app for their insulin pumps in the US (Tandem 2022). One of the latest technologies within diabetes treatment launched in Norway is called *closed loop*. Closed loop refers to compatible insulin pumps and CGMs communicating through Bluetooth, where the measurements from the CGM are interpreted by an algorithm that determines the insulin injections from the pump, imitating healthy, functioning pancreas (Diabetesforbundet 2021; Klonoff, Shang, and Zhang 2021; Saltzstein 2020).

Both insulin pump and CGM data can be uploaded to the equipment manufacturer's software or Diasend, which are cloud-based data management platforms for diabetic patients and diabetes healthcare personnel. The primary purpose of this software is to make diabetic lives and healthcare personnel’s work easier by optimizing diabetes management and patient care (Cleveland and Haddara 2021; Diasend 2020).

2.2.2 Continuous Glucose Monitoring

Traditionally, glucose levels were controlled by blood samples several times a day, typically collected by puncturing the fingertip (Istepanian et al. 2011). This constant puncturing of skin has been described as a dreadful experience by many patients, as it has been painful and led to skin inflammations (Cleveland and Haddara 2021). Continuous glucose monitoring (CGM) is an advanced method to monitor glucose levels in real-time at regular intervals that translate the measures into data and information about glucose direction and rate of change. A sensor attached to the patient’s body with an adhesive patch consists of a transmitter with a tiny sensor wire inserted just under the skin in the subcutaneous fat using an automatic applicator. CGM offers great relief to many patients, as skin puncturing only occurs when the sensor is being applied every week or so (the life span of each CGM varies by model). The transmitter communicates wirelessly with a connecting receiver and transfers real-time glucose data, usually via Bluetooth. Most sensors can display measurements both in an app and a PMD (Cleveland and Haddara 2021; Dexcom 2022; Islam et al. 2015; Saltzstein 2020). The sensor notifies through an alarm in the receiver device when the glucose levels are getting too high or too low and can be customized to each patient’s individual thresholds (Britton and Britton-Colonnese 2017; Diabetesforbundet 2021). Over the last 20 years, they have continuously been developed and improved to become longer-lasting, more accurate, and smaller in size (Cleveland and Haddara 2021; Rodbard 2016).

The use of CGM is associated with real-time monitoring of glucose levels that can lead to timely intervention of hypo- and hyperglycemic episodes and improving the glycated hemoglobin A1c (HbA1c) (Al-Taee et al. 2015; Diabetesforbundet 2021; Rodbard 2016). Due to proactive monitoring using CGM, statistics show that patient’s long-term complications can be reduced between 40% and 75%, and clinical studies have shown a glucose level reduction of 2 points on average by the use of CGM (Britton and Britton-Colonnese 2017; Cleveland and Haddara 2021; Longva and Haddara 2019). The Norwegian health government advises that all patients with type 1 diabetes should be considered for CGM, especially patients who experience fluctuating glucose levels, live alone, or have reduced ability to feel symptoms of hypoglycemia (Diabetesforbundet 2021).

2.2.3 The Big Data of Healthcare

As the cost of healthcare has increased alarmingly over the years, healthcare institutions look for possible ways to lower the costs while still improving patient care. Patient monitoring and wearable IoT devices give a foundation for Big Data in healthcare, which emerges as a plausible solution for transforming the healthcare industry even further (Alvarez, Baller, and Walton 2021; Patil and Seshadri 2014). Big Data in healthcare is generated by healthcare records, medical sensors, clinical data, healthcare apps, etc., and the amount available is tremendous (Bide and Padalkar 2020; Islam et al. 2015; Rehman, Naz, and Razzak 2021). The term "Big Data" refers to the rapidly growing, large, and complex data sets exceeding traditional computational, storage, and communication capabilities. (Patil and Seshadri 2014). Big Data is characterized by *the five Vs*; *Volume* (it holds a large quantity of patient data), *Variety* (it contains a variety of data types, such as patient information, clinical data, prescriptions, etc.), *Velocity* (the different pace of data being generated, e.g., glucose measurements have medium-velocity while doctor notes are at rest), *Value* (the data's benefit for the healthcare ecosystem), and *Veracity* (the data's quality and reliability) (Rehman, Naz, and Razzak 2021). By utilizing the power of Big Data analysis with real-time patient measurements and clinical data, healthcare personnel could make evidence-based decisions on treatments which will be crucial for patient care. However, it also significantly increases privacy and security concerns. Handling the vast amount of data and anticipating risks by integrating technology is essential (Bide and Padalkar 2020; Patil and Seshadri 2014; Rehman, Naz, and Razzak 2021). Due to this, Alvarez, Baller, and Walton (2021) state that the discussion of who owns the data generated from healthcare IoT is of imminent concern and suggests that healthcare institutions must prepare to discuss privacy and security challenges.

2.3 Privacy and security

Even though the use of wearable IoT devices, such as insulin pumps and CGMs, is growing and offers a lot of possibilities in the healthcare sector, benefiting both patients and healthcare personnel, it does not exist without challenges. It is therefore still not fully adopted in the entire sector. Some of the main challenges pointed out concern patient privacy and security, access control, and data storage and management (Abdollahi, Moghaddam, and Parvar 2019; Alaba et al. 2017; Armstrong et al. 2016; Longva and Haddara 2019). As it deals with vital, sensitive medical data that is extremely valuable on the black-marked and can be accessed through global information networks, IoT is an attractive target for cyberattacks (Alaba et al. 2017; Islam et al. 2015; Lerman 2020). Medical information or IT systems that are manipulated or blocked for patients and healthcare personnel to access threaten the patients' safety and can result in death (Riksrevisjonen 2020). Critical gaps are found in current healthcare IoT, in how patient information is collected and transferred within and across healthcare institutions and shared among healthcare personnel. Human errors, authentication processes, and data integrity have been discussed as potential risk factors (Longva and Haddara 2019). Patient privacy and information security are fundamental aspects that need to be considered when dealing with healthcare technology. Still, due to the complexity of IoT functionality, non-functional requirements, such as privacy and security, have not received sufficient attention despite it being critical to the successful growth of medical IoT (Alhirabi, Rana, and Perera 2021; Armstrong et al. 2016; Rehman, Naz, and Razzak 2021). In general, the healthcare sector lacks sufficient security to prevent cyberattacks and contain patient privacy. No unified standard policy regarding privacy exists, and solutions are challenging to find due to IoT environmental attributes. However, patient privacy must be guaranteed, as patients require maximum protection for their medical and personal information. Therefore, medical device and technology companies need to improve their security approaches to ensure cybersecurity and guarantee confidentiality, access control, and privacy for patients and devices (Alaba et al. 2017; Armstrong et al. 2016; Britton and Britton-Colonnese 2017; Kintzlinger and Nissim 2019; Patil and Seshadri 2014; Riksrevisjonen 2020). Patil and Seshadri (2014) further argue that traditional security solutions cannot be applied to the Big Data generated by IoT. As the healthcare industry continues leveraging Big Data technologies for healthcare analytics, there is a need for data governance to regulate and manage healthcare data. Diabetes data, such as glucose levels and insulin injections, will be registered, saved, and most likely shared using IoT in diabetes treatment. It is therefore crucial that the device providers and healthcare institutions issuing these devices have and follow protocols to keep the information safe (Diabetesforbundet 2021). All stakeholders in the healthcare sector are responsible for ensuring the security and privacy of patients and their information (Rehman, Naz, and Razzak 2021), but according to The Office of the Auditor General, in Norway, the healthcare institutions are juridic responsible for handling medical information about their patients. Yet, they experience the institutions and their personnel lack knowledge about patient privacy and information system security (Riksrevisjonen 2020). Healthcare personnel play an essential role in guiding patients in recommending equipment, demonstrating best usage practices, and cautioning potential limitations. Thus, despite the limited time in the healthcare sector, it is argued that personnel should ensure they stay informed and regularly check resources to learn more about the pros and cons of the technology, such as potential disadvantages like cybersecurity risks (Ahn and Stahl 2019).

The importance of preserving privacy in IoT has been confirmed by the GDPR, which applies to all systems dealing with personal data (Alhirabi, Rana, and Perera 2021). The European General Data Protection Regulation (GDPR) aims to ensure more meaningful and robust data protection rights for individuals by allowing users of technology to control their collected data and know how it is collected, requiring more transparency and openness from the organizations handling the data. It has been suggested as a solution for improving user privacy in IoT (Barati and Rana 2020; Loideain 2019). Three essential roles are defined in GDPR; (1) *the data subject*, which is identified through an identifier (the patient identified through, e.g., their name or personal ID), (2) *a controller*, an institution determining what operations will be executed on the collected data, and (3) *a processor* that is responsible for processing personal data on behalf of the controller (Barati and Rana 2020). Due to the generation of Big Data and continuously changing and increasing risks, controllers must regularly assess and review potential vulnerabilities (Loideain 2019). According to GDPR, controllers have the responsibility if processing of data is violated and share responsibility with the processor when the subject has no direct control of the processing steps of their personal data (Barati and Rana 2020). Successful implemented GDPR relies on the capacity of data controllers to monitor compliance by all IoT stakeholders to their obligations, regulators' ability to identify if processors are making significant decisions, and the stakeholders' ability to undertake the responsibilities and meet critical requirements of GDPR provided by the authorities (Loideain 2019). The confidentiality of medical information is ensured through these laws and regulations, but data stored in apps are often stored on remote servers, which are more vulnerable to security breaches (Ahn and Stahl 2019). In addition to GDPR, the newly decided Schrems II judgment addresses cross-border data flows by putting pressure on companies to keep the data inside the EU and seeks to ensure the safety of personal data being transferred (Chander 2020; Datatilsynet 2020).

Many companies lack transparency regarding data collection, storing, handling, and who has access to it, and use unclear and avoidant language in their privacy policies. Additionally, there have been incidents where sensitive data has been transmitted without encryption and sold without the patient's knowledge (Alvarez, Baller, and Walton 2021). Unfortunately for diabetes patients, they are faced with accepting these privacy policies if they want to be able to use the devices and technology. The majority of diabetes technology companies state that they gather user information such as IP addresses, Internet Service provider, web browser or iOS-version, other information related to the computer or phone applications, and location. In addition, they gather data related to the user's activity while using their services and products. Further, they claim all personal information is anonymized, without elaborating how this process is done, and argue the data can be used for any purpose as long it is not identifiable (Britton and Britton-Colonnese 2017; Cleveland and Haddara 2021). The principles of GDPR are not required if the personal data collected from an IoT device is anonymized so that the individual is no longer identifiable. However, there are techniques for re-identifying data, where identifiable information is extracted from anonymized data (Alvarez, Baller, and Walton 2021; Loideain 2019).

Although IoT has become widely integrated within the healthcare sector, little attention is paid to patient and healthcare personnel's awareness and knowledge of data handling, privacy, and security (Alvarez, Baller, and Walton 2021). According to Atzori, Iera, and Morabito (2010), people will resist IoT adoption as long as there is no public confidence that it will not cause violations and threats to their privacy. Potential lack of trust, where the patients do not want their data to be shared or recorded in fear of it not being kept safe and confidential, poses a risk for the patient's further treatment and clinical outcome and may deprive healthcare personnel and researchers of important information that can benefit the society (Britton and Britton-Colonnese 2017; Rehman, Naz, and Razzak 2021). However, previous studies have found that diabetes patients using wearable IoT are willing to share their diabetes data, despite significant privacy concerns and data leaks featured in the media in recent years, indicating a lack of awareness of cyberthreats or overestimating the internal protection of IoT devices. The leading factor for cyber behavior was found to be personal experience, suggesting that if patients have not experienced cyberattacks, they are more likely not to be concerned about privacy and cyberthreats (Alvarez, Baller, and Walton 2021; Cleveland and Haddara 2021).

2.3.1 Cyberthreats and vulnerabilities

Patient safety is fundamental in the Norwegian healthcare sector, and with the increasing digitalization affecting this sector, cybersecurity is becoming a more prominent aspect of healthcare (Norsk helsenett 2021). However, the healthcare sector is always going to be in a difficult position where the focus of helping people get better and ensuring cybersecurity generates has to be balanced (Fearn 2021). Even though laws and regulations exist, they are inadequate and fail to prevent cyberattacks (Kintzlinger and Nissim 2019). During the past decade, the healthcare sector has experienced a steady increase in security breaches (Patil and Seshadri 2014). Norwegian National Cyber Security Centre (NCSC) reports that sectors with a critical society function, such as the healthcare sector, are at greater risk for cyberattacks. There were reported three times as many severe cyberattacks in Norway in 2021 as in 2019, and during the last year, cybercrime has increased by 72%, which is by far a much steeper increase than the average 40% worldwide. On a weekly average there is 458 cyberattacks in Norway (Nasjonal Sikkerhetsmyndighet 2022; Seglsten 2021). Norsk helsenett estimate a 90% chance of all organizations within the Norwegian healthcare sector to experience a cyberattack for financial gain, another 90% chance of advanced cybercriminals trying to access medical data and personal information, and a 60-90% chance of cyberattacks affecting IT infrastructure and patient care (Norsk helsenett 2021). The healthcare sector is an interesting target for cybercriminals, industry espionage, and government intelligence with the intention to steal, manipulate, interfere with, or affecting data or operations. The tactics and approaches of cybercriminals evolve and change rapidly, making it challenging for the healthcare sector to keep up and prevent cyberattacks. A cyberattack in the healthcare sector can cause great consequences for patient care; threaten patient privacy and security, and in worst-case result in life-threatening situations (Putch 2021; Riksrevisjonen 2020). With the ever-changing risk environment and new emerging threats, there is no reason to believe cyberattacks against the healthcare sector will slow down any time soon (Fearn 2021; Patil and Seshadri 2014). Kintzlinger and Nissim (2019, 11) define cyberattack in the context of PMDs as any attempt to gain unauthorized access and (1) destroy, disable, alter, or steal data, or (2) destroy, disable, alter therapy configurations, or (3) compromise a patient's healthcare. Due to its connectivity and variety of components, vulnerabilities, and risks, the medical IoT ecosystem is an attractive target for cyberattacks. Insulin pumps are revealed to be one of the most vulnerable PMDs, as with its wide range of functionality and integrations generally is more complex than other PMDs' and are exposed to 88,2% of the attacks. It can by different degrees be affected by a range of attack against hardware (such as Bluetooth and sensor nodes), network (wired and wireless), and smart application (such as apps and software), such as hacking, data manipulation, DoS, ransomware, equipment hijacking, cyberattacks causing insulin dose change, or measurement distribution (Alaba et al. 2017; Kintzlinger and Nissim 2019). According to Amaraweera and Halgamuge (2019), most threats occur due to impersonation, data breaches, and unauthorized access. By attacking medical IoT, the cybercriminal can get access to and control over real-time communication, capturing sensitive patient data and sending fake information and instructions to devices in the network, as the limited computational power limits the encryption possibilities in IoT, leaving the devices open and exposed to hackers (Alaba et al. 2017; Islam et al. 2015). One example of an attack affecting diabetes IoT is from 2016, where a security flaw for an insulin pump and CGM was discovered; hackers could have remotely hijacked the communication and programmed commands to inject more insulin into the patient's body, which in worst-case could end the patient's life (Britton and Britton-Colonnese 2017; Kintzlinger and Nissim 2019). The first direct correlation between a cyberattack and human death was reported at the University Hospital of Düsseldorf Germany in 2020. The hospital was hit by ransomware that blocked the hospital's IT systems from admitting more patients, causing a patient to die in transit to another hospital because the emergency room allegedly was closed (Putch 2021). A simulated cyberattack performed by the Office of the Auditor General of Norway revealed severe breaches and shortcomings in the four Regional Health Authorities in Norway's cybersecurity. Through the simulated attacks, they were able to access several critical systems and databases and gain control over the IT infrastructure, and would have been able to delete, manipulate and steal great amounts of sensitive health data and personal information (Kjærnli 2021; Riksrevisjonen 2020). Additionally, they discovered that a lot of the patients' medical information were available for a staff that were not associated with the individual patient's case and would not be needing it. Only one of the four healthcare regions were able to detect some of the activities in the simulation (Riksrevisjonen 2020).

Even though privacy and security are more in focus than before, the continuous technological development and lack of sufficient knowledge and competence on security is increasing digital risks. Security measures are not timely implemented and does not match the actual threat situation, leaving the gap between threats and the level of security in Norway to surge. Therefore, IT security needs to be strengthened in Norwegian institutions, and leaders must take responsibility to ensure this. In order to do so, they should turn to sectors that have been working with security and risk evaluation for decades, such as The Norwegian Armed Forces and finance sector, to learn how to rise the competence level within their institution (Alvarez, Baller, and Walton 2021; Britton and Britton-Colonnese 2017; Nasjonal Sikkerhetsmyndighet 2022). The Norwegian Electrotechnical Committee (NEK) claim that by implementing ISO/IEC 27001, most organizations and institutions in Norway can strengthen their cyber defense, as it offers guidance to handle risks, threats and vulnerability, and keep confidentiality and integrity in regards to information security (Kjærnli 2021). A certification in ISO/IEC 27001 proves the technology provider follow best practice and adheres the highest data security standards. It is the most acknowledged standard for information systems internationally, as it is provided by an independent third-party (DNV 2022). Healthcare personnel's attitude towards and knowledge of privacy and security is one of the main reasons the Office of the Auditor General of Norway were able to access as much of the systems as they did. They reported that the personnel are weakening the security by using weak passwords, sharing access, and sharing more than what is necessary to perform a task. They were also found likely to click on links in fake e-mail that would install virus (Riksrevisjonen 2020). To keep patients, their data, and healthcare IT systems safe, healthcare institutions should make sure only authorized personnel have access to systems and patient information, continually educate and remind people of the importance of good safety routines and worst-case scenarios and making two-factor authentication (2FA) for accessing a system mandatory, which adds more protection layers to the systems and reduces the risk of attack through password. By educating healthcare personnel in security hygiene and password best practice the reuse and use of weak passwords and password sharing can be reduced (Greene 2020). Education about cybersecurity happens through e-learning annually, but as it is not customized to individual work groups' routines and challenges it is hard for healthcare personnel to apply theory to practice (Riksrevisjonen 2020).

3. Research method

According to Oates (2006, 7), *"research is the creation of new knowledge, using an appropriate process, to the satisfaction of the users of the research"* and is distinguished between quantitative and qualitative research. Quantitative research seeks to find patterns in numbers, draw conclusions based on statistics, and is great for answering questions like "how many" and "what". Qualitative research analyzes non-numeric data, like interviews and documents, and is great for answering questions like "why" and "how", exploring and creating a holistic view of social problems (Myers 1997; Oates 2006). In this dissertation, a qualitative approach was selected.

This chapter presents an overview of the research approach, and provides descriptions of the adopted research design, including the data collection and analysis methods. Figure 3-1 illustrates the research process by Oates (2006), and summarizes the research design adopted for this dissertation, marked in red circles.

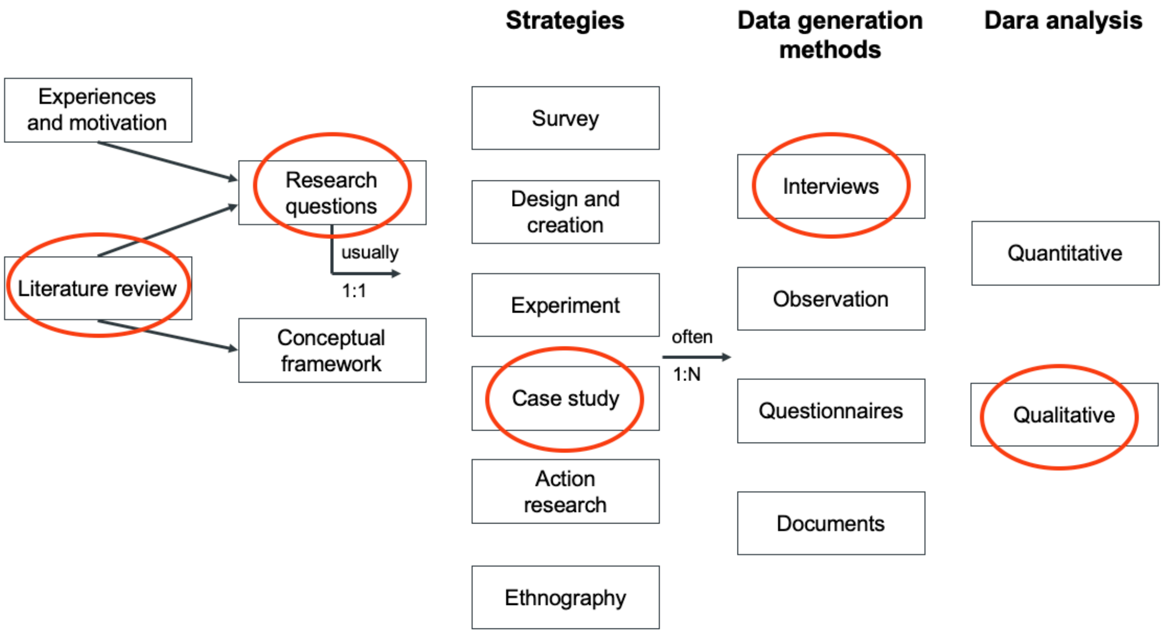

Figure 3-1: The research process by Oates (2006, 33).

3.1 Research strategy

This research aims to identify new insights into how the use of IoT in diabetes treatment affects patients' life-quality and how the assumed increased life-quality is weighed against potential cyberthreats related to IoT. Thus, it was decided to apply an exploratory research approach to answer the research questions. According to Yin (2018), an exploratory research method is satisfactory for investigating and explaining why certain phenomena occur. Exploratory research is frequently used when the available literature about the topic in focus is limited and could help identify topics for future research (Oates 2006). This research was carried out through a literature review and multiple-case study research (Yin 2018).

Literature reviews represent an essential element in all research and are a well-established method for accumulating existing knowledge and identifying research gaps within the topic of focus. By critically reviewing key articles in the field, the researcher will be able to determine what is known about the topic, controversies, potential clashes of evidence, and who the key contributors to research on the topic are. When conducting a literature review properly, the researcher will be able to link current research questions, findings, and discussions to the existing literature and demonstrate their credibility and contribution to research (Bryman 2012; Yin 2016).

When research is based on subjective perceptions, and there is little to no control over behavioral events, Myers (1999) and Yin (2018) recommend using a multiple-case study. Case studies are characterized by focusing on depth rather than breadth. As there is no consensus on what a case is, they can include analysis on individuals, groups, organizations, communities, etc., or anything studied holistically through one or more research methods in order to obtain as many details as possible when investigating an aspect of real-life contexts, such as an information system or organization (Conde 2021; Thomas 2021; Walsham 1995). The analytical results of a multiple case study (two or more cases) are likely to be more compelling and prevail over those from single-case studies, therefore, multiple-case study is often favored over a single-case study. It should be mentioned that multiple-case studies have disadvantages, as it can demand extensive time and resources, making it challenging for a single student or independent researcher (Yin 2018), however, due to the limited timeframe and focus on the current situation for this research it is classified as a short-term, contemporary study (Oates 2006).

A combination of literature review of the existing knowledge and interviews with the different stakeholders can generate data that, through careful analysis, will give a holistic view of the topic in focus (Kaplan and Duchon 1988; Oates 2006). The empirical part of this study consists of semi-structured interviews with the three stakeholder groups that make the cases: (1) diabetes patients, (2) healthcare personnel, and (3) industry representatives. The analysis will be based on the stakeholders' perceptions of the privacy and security related to diabetes IoT wearables in Norway and aim to provide new insight into how the Norwegian industry and future research can address challenges that are assumed to be revealed (Yin 2018).

3.2 Data collection

The data collection process lasted from October 2021 until April 2022. This research used two qualitative data collection techniques: literature review and interviews. Collected data consists of journal articles, government reports and documents, industry blog posts, and interviews with central Norwegian stakeholders. The techniques are presented in more detail in the sections to follow.

3.2.1 Literature review

Secondary data were collected between October and December 2021, and in late April 2022, through a literature search in various databases and government websites, tracing relevant cited articles within identified articles, and searching in industry blogs. Some literature was collected over the past three years as parts of previous exams and course curriculum.

The literature period was set between 2010 and April 2022. Initially, the literature search targeted "The Basket of eight," the leading journals within Information Systems (Cleveland and Haddara 2021); however, few relevant publications were identified. Further, literature searches were conducted in the diabetes-specific Journal of Diabetes Science and Technology and the American Diabetes Association's database diabetesjournals.org, which offered several potential articles. Lastly, a search was performed in Google Scholar, including all journals and conferences within medicine, information systems, and technology. During the collection process, the journal's impact factor, the paper's citations relative to the year of publication, and the overall number of author's citations were considered the most reliable research. For the literature search, the keywords "Internet of Things", "Healthcare", "diabetes", and "Cybersecurity" were used in different forms and combinations with the keywords "hacking", "patient monitoring", "CGM", "e-health", "privacy", and "GDPR".

Additionally, Norwegian government websites and industry blogs were searched for healthcare technology and cybersecurity reports and news. In total, 98 articles, reports, and blogposts were identified and collected, then the abstracts and summaries were skimmed through to check their relevance for this research. When the potential literature was selected, it was carefully read to identify existing knowledge and the main themes discussed in the existing body of knowledge. For this thesis, 42 articles, reports, and blogposts are included as the theoretical background. Table 3-1 provides an overview of the selected literature. Some fall under more than one theme or topic based on their focus and scope. Combined, this literature offered guidance for formulating the problem definition and the interview guides.

Main theme	Topic	Literature
IoT technology		(Alaba et al. 2017; Alhirabi, Rana, and Perera 2021; Barati and Rana 2020; Gubbi et al. 2013; Islam et al. 2015; Perera et al. 2014)
IoT in healthcare	Patient monitoring	(Abdollahi, Moghaddam, and Parvar 2019; Alvarez, Baller, and Walton 2021; Bhatt and Bhatt 2017; Chouffani 2020; Cleveland and Haddara 2021; Gómez, Oviedo, and Zhuma 2016; Islam et al. 2015; Kintzlinger and Nissim 2019; Lerman 2020; Longva and Haddara 2019; Patil and Seshadri 2014; Saltzstein 2020)
	Diabetes treatment	(Abdollahi, Moghaddam, and Parvar 2019; Ahn and Stahl 2019; Al-Taee et al. 2015; Britton and Britton-Colonnese 2017; Cleveland and Haddara 2021; Diabetesforbundet 2021; Islam et al. 2015; Istepanian et al. 2011; Klonoff, Kerr, and Kleidermacher 2017; Klonoff, Shang, and Zhang 2021; Longva and Haddara 2019; Rodbard 2016; Saltzstein 2020)
	Big Data	(Alvarez, Baller, and Walton 2021; Bide and Padalkar 2020; Islam et al. 2015; Patil and Seshadri 2014; Rehman, Naz, and Razzak 2021)
e-health challenges	Privacy, security & Data management	(Ahn and Stahl 2019; Alaba et al. 2017; Alhirabi, Rana, and Perera 2021; Alvarez, Baller, and Walton 2021; Atzori, Iera, and Morabito 2010; Barati and Rana 2020; Britton and Britton-Colonnese 2017; Chander 2020;

		Cleveland and Haddara 2021; Datatilsynet 2020; Kintzlinger and Nissim 2019; Lerman 2020; Loideain 2019; Patil and Seshadri 2014; Rehman, Naz, and Razzak 2021; Riksrevisjonen 2020; Saltzstein 2020; Shahid et al. 2022)
	Cyberthreats & attacks	(Alaba et al. 2017; Alvarez, Baller, and Walton 2021; Amaraweera and Halgamuge 2019; Armstrong et al. 2016; Fearn 2021; Greene 2020; Kintzlinger and Nissim 2019; Kjærnli 2021; Nasjonal Sikkerhetsmyndighet 2022; Norsk helsenett 2021; Patil and Seshadri 2014; Putch 2021; Riksrevisjonen 2020; Seglsten 2021)

Table 3-1: Overview of selected literature.

3.2.2 Interviews

Interviews were conducted between February 2022 and mid-April 2022. Interviews are a suitable data generation for research that focuses on obtaining detailed information by asking complex and open-ended questions, exploring experiences that cannot easily be observed, and accessing informants' interpretations in the field (Oates 2006). This research has conducted individual semi-structured in-depth interviews. Semi-structured interviews allow for more flexibility. It is performed more like a natural conversation where the informant can feel more comfortable and talk more openly about the topic, and questions can be adjusted for themes and issues or follow-up questions that are particularly interesting and not prepared for. Individual in-depth interviews are well suited for gaining the respondent's honest personal experience without the influence of others (Bryman 2012; Gripsrud, Olsson, and Silkoset 2016).

When doing a case study, there is a need for some structure to ensure comparability between the groups (Bryman 2012). Hence, interview guides based on the current knowledge identified in existing literature were developed to ensure all relevant questions for this research were covered (Appendix C - E). As there were three stakeholder groups, three interview guides were designed with specific adjustments for each group. The interview guides were developed, and questions were formulated following the guidelines of (Bryman 2012) and (Oates 2006); formulate open questions that are not too specific to help answer research questions, do not ask leading questions, create a logical order of the questions to ensure flow in the conversation, and use language that is comprehensible to the informant.

As patient and healthcare personnel interviews were scheduled to last up to one hour, they were recorded to obtain as much information as possible when transcribing and ensure no important details were missed. Industry interviews were scheduled for up to 15 minutes. Therefore, it was decided not to record them as it would be possible to grasp the essential details by transcribing them straight after the interview. All stakeholders have been anonymized, the ethical considerations are described in the last section of this chapter (3.5).

All interviews were carried out in Norwegian to avoid language barriers, as it is both the author's and stakeholders' spoken language (except for one stakeholder whose spoken language is Swedish, which is closely related to Norwegian and therefore was considered not to be affected by any language barrier). Transcripts were written in Norwegian, the essence and the main findings were translated to English.

3.2.3 Case selection: The stakeholders

According to Oates (2006), non-probability techniques can be applied when the researcher does not know much about the population. It is not adequate for generalization but can provide a basis when time and resources are limited. The case selection process in this research employed a combination of strategies: purposeful sampling (the sample is chosen based on being likely to produce valuable data and offer depth to the phenomenon), snowball sampling (one person in the targeted sample suggest another relevant person outside the sample), and convenience sampling (the sample is chosen based on being easy to reach and likely to participate) (Oates 2006; Patton 2015). This study followed a grounded theory approach, which emphasizes both the emergence of theoretical categories from evidence and an incremental approach to case selection and data gathering. The data collection can be closed when data saturation is achieved, meaning the point where the observing phenomena has been seen before (Eisenhardt 1989). As the aim of the study was to investigate in as much depth as feasible, and theory building research allows for adding and altering data collection methods during the study if it is likely to provide new theoretical insight or to better ground the theory, some samples were added during the study (Eisenhardt 1989; Oates 2006). Due to the limited time scope for this research, it was decided not to continue sampling when getting declined or not replied when contacting potential participants. However, for the first two cases, data saturation was achieved after the third interview in each case. The third case could have benefited from being divided into further three cases, adding more participants in each case, to ensure data saturation. This is addressed in section 6.2 Limitations and future research.

3.2.3.1 Stakeholder group: Diabetes patients

Diabetes patients were included in the study as they are the ones actively using the technology of question and would contribute with first-hand information on how it affects their life-quality and possible concerns they have. The recruiting process for patients started in November 2021, using the purposeful and convenience sampling techniques, by reaching out to know type 1 diabetes patients within the researcher's network and asking for an hour-long video conferencing interview. This also led to snowball sampling, as one of the patients knew about another that might be willing to participate. To participate, the patients had to fulfill the following criteria: (a) have been diagnosed with type 1 diabetes, (b) have previously been using manual diabetes equipment, and (c) are currently using CGM and/or insulin pump. In total, six potential stakeholders were contacted, and only one could not participate due to not fulfilling the criteria. By mid-January 2022, five stakeholders were identified and scheduled for interviews throughout February.

Each interview was conducted as a semi-structured interview following the interview guide for patients (Appendix C). The questions were directed toward: (I) how the patient experience their diabetes, (II) how the patient experience using IoT technology in diabetes treatment, and (III) the patient's perceptions regarding privacy and security related to using this technology. The interviews lasted between 30 and 60 minutes, depending on the patient's elaboration on each question and topics that were not prepared for. Data saturation was achieved by the third interview. Table 3-2 shows an overview of the participating diabetes patients. Patient identity is replaced with the letter P and a number in the order of when the patient interviews were conducted.

Diabetes details	**P1**	**P2**	**P3**	**P4**	**P5**
Gender	Male	Female	Female	Female	Female
Age when diagnosed	40 years	17 years	9 years	3 years	5 years
Lived w/diabetes	18 years	16 years	15 years	26 years	23 years
Using dia. IoT	6 months	8 years	8 years	8 years	6 years
Current CGM	Guardian sensor 3	FreeStyle Libre 2 + app	Dexcom G6 + app	Dexcom G6 + app	Dexcom G6
Current insulin pump	Medtronic MiniMed 780G	Omnipod Dash	Tandem t:slim X2; Control-IQ	Omnipod Eros	Tandem t:slim X2; Basal IQ

Table 3-2: Overview of participating diabetes patients.

3.2.3.2 Stakeholder group: Healthcare personnel

Healthcare personnel were included as they could contribute with the medical perspective on how IoT affects patient life-quality and how they are handling privacy and security-related concerns and challenges. The recruiting process for healthcare personnel started in December 2021, using the purposeful sampling technique, by reaching out through e-mail to Norwegian institutions specializing in diabetes treatment, asking for an hour-long video conferencing interview with nurses and doctors. To participate, the healthcare personnel had to fulfill the following criteria: (a) be a nurse or a doctor mainly working with diabetes patients, and (b) work with patients using CGM and insulin pumps. In total, seven healthcare institutions were contacted. Some were unable to participate due to limited time and resources, and others did not answer. One organization replied within a few days that they were willing to participate. By the beginning of February 2022, five healthcare personnel were identified and scheduled for interviews throughout February and March.

Each interview was conducted as a semi-structured interview following the interview guide for healthcare personnel (Appendix D). The questions were directed toward: (I) how the healthcare personnel experiences the use of IoT in diabetes treatment and (II) the healthcare personnel's perceptions regarding privacy and security related to the use of this technology. The interviews lasted between 30 and 60 minutes, depending on the healthcare personnel's elaboration on each question and topics not prepared for. A second organization replied after the first organization was scheduled for interviews. This second organization required an application to be submitted to consider their participation. The data collection process was already started, and data saturation was achieved after the three first interviews already scheduled; due to this, the second organization was not included. Table 3-3 shows an overview of the participating healthcare personnel. Healthcare personnel identity is replaced with the letters HCP and a number in the order of when the healthcare personnel interviews were conducted.

Professional details	**HCP1**	**HCP2**	**HCP 3**	**HCP4**	**HCP5**
Gender	Female	Male	Female	Female	Female
Role	Diabetes nurse	Diabetes doctor	Diabetes nurse	Diabetes nurse	Diabetes doctor
Type of organization	Outpatient Clinic	Outpatient Clinic	Outpatient Clinic	Outpatient Clinic	Outpatient Clinic
Working w/diabetes	22 years	30 years	11 years	7 years	13 years
Working w/dia. IoT	12 years	20 years	11 years	7 years	12 years

Table 3-3: Overview of participating healthcare personnel

3.2.3.3 Stakeholder group: Industry representatives

The sample of industry representatives is more diverse than the two aforementioned and is therefore divided into three sub-categories. (1) Medical equipment and healthcare technology company representatives were included, as they would contribute with insights into how their organization and technology is handling patient data and ensuring patient safety. (2) The Norwegian government was included as they would contribute with information about the general cyberthreat level and challenges related to e-health and the healthcare sector, and what considerations are taken when approving medical technologies. (3) Representatives from legal consulting within healthcare technology were included as they would contribute to the legal aspect of IoT use and data handling in the healthcare sector. In general, this group of industry representatives was included in the case selection to get the industry perspective to verify or refute potential concerns in the other two groups.

The recruiting process for industry representatives started in March 2022, using the purposive sampling technique, by reaching out through e-mail to relevant representatives found through researching the different company and government websites, asking for a 15-minute phone call interview. This also led to snowball sampling, where some of the stakeholders offered to forward the e-mail to others they thought would be a match for the research topic and willing to participate after participating themselves. The criteria for industry representatives to participate was that they had to be an authority for making a statement within their industry. In total, ten e-mails were sent to recruit this stakeholder group. Some were unable to participate due to legal reasons; others did not answer. Four interviews were scheduled and conducted consecutively as representatives replied and were completed by mid-April. One representative asked to receive the questions by e-mail and responded with a brief statement on the questions they deemed relevant to their area of expertise.

Each interview was conducted as a semi-structured interview following the interview guide for industry representatives (Appendix E). As there are three subcategories within this stakeholder group, the questions in the interview guide were used in different combinations and variations, customized to each sub-category and the representative's position. The questions were directed toward: (I) how data generated by diabetes technology is handled, (II) challenges regarding privacy and security for diabetes technology, and (III) cyberthreats related to diabetes technology, e-health, and the healthcare sector. The interviews lasted between 10 and 20 minutes, depending on the industry representative's elaboration on each question and topics that were not prepared for. Table 3-4 shows an overview of the participating industry representatives. Industry representative identity is replaced with the letters IR and a number in the order of when the industry interview interviews were conducted.

Professional details	**IR1**	**IR2**	**IR3**	**IR4**	**IR5***
Gender	Male	Male	Female	Male	Male
Industry	Government	Medical devices and healthcare company	Medical devices and healthcare company	Legal consulting	Government
Position	Head of data security	Product Manager	Privacy director	Legal adviser	Senior advisor
Category	e-health	Diabetes equipment	Diabetes equipment	GDPR	Medical equipment

Table 3-4: Overview of participating industry representatives.
**Industry representative 5 answered questions by e-mail.*

3.3 Data analysis

According to Bryman (2012), one of the main difficulties with qualitative research is that it rapidly generates a large amount of data. Qualitative data is attractive due to its richness, yet this richness makes it challenging to make sense of and find analytic paths (Patton 2015). There are few well-developed and widely accepted rules and recipes for analyzing qualitative data and case studies, causing many researchers to become stalled at the analytical stage. Yet, there are broad guidelines for preparing, coding, and analyzing qualitative data (Bryman 2012; Yin 2018). Additionally, Patton (2015, 762) states the most important thing is to sincerely try to "fairly represent the data and communicate what the data reveal given the purpose of the study". How to interpret this study's findings has been carefully evaluated, and it was decided that a cross-case analysis would be suitable. Figure 3-2 demonstrates how the data was collected and analyzed.

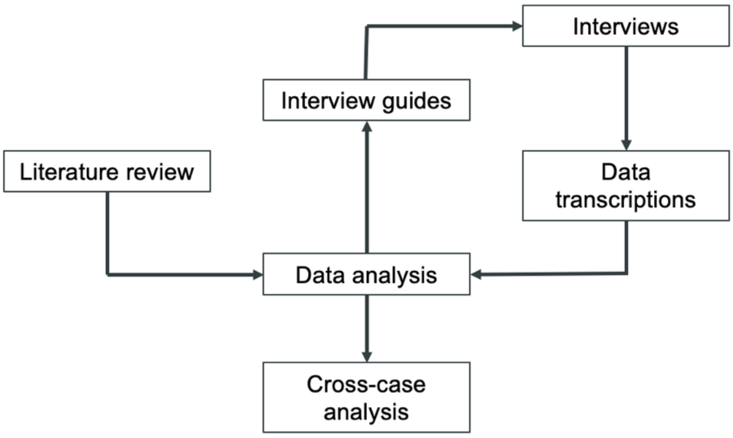

Figure 3-2: Data collection and analysis overview.

3.3.1 Data preparation

After obtaining consent, the interviews with patients and healthcare personnel have all been digitally recorded. The consent form can be found in Appendix A. Recordings help remove potential bias and errors and obtain as much information as possible, as relying on notes and memory can be difficult (Oates 2006). They can, however, be disadvantageous as it takes time to transcribe and extract a set of useful data from it (Walsham 1995). Even so, they can be rewarding as they bring the interview back to life, providing the researcher a chance to start thinking about and analyzing the data (Oates 2006). Keeping the advantages in mind, the interviews were recorded as they were scheduled to last up to an hour, then transcribed manually.

It was decided not to record the interviews with industry representatives as these were scheduled to last 15 minutes. There were two reasons for this; (1) When it got clear that industry representatives should be included as a stakeholder group in this study, the application for NSD was already submitted and approved. Due to the limited time scope of this research and time running out, it was considered too risky to wait for a review of the application for another approval of interview recordings. And (2), by taking notes during the interview and transcribing them straight after the phone call, the researcher considered it manageable to attain all information. Therefore, notes were carefully taken during the interviews and transcribed immediately after.

3.3.2 Cross-case analysis

This case study aims to understand, explain, and answer the "how" and "why" questions regarding the use of IoT in diabetes treatment, its effect on patient life-quality, and challenges related to cyberthreats and data management. As the purpose is to synthesize the findings and results across the different stakeholder groups and consequently give a holistic view of the case, a cross-case analysis was conducted. According to Patton (2015), cross-case analysis is suitable for analyzing and identifying patterns and themes across the multiple-case study. By analyzing patterns across interview questions, responses, and participant groups, the goal is to retain the integrity of the case and then compare these within-case patterns across the cases in a cross-case analysis and develop ideas for further study (Patton 2015; Yin 2018).

The primary sources of data analyzed were the interview recordings and transcriptions. Similarities and contrasts within each case (stakeholder group) were identified and categorized according to the topic of discussion. Further, the cross-case analysis investigated the similarities and differences between the cases, focusing on how the use of IoT in diabetes treatment was perceived in terms of (1) the effect on patient life-quality, (2) patient privacy and security, and (3) cyberthreats towards the healthcare sector. The results and findings from the cross-analysis were compared with findings from the literature and are presented in the discussion chapter (chapter 5).

3.4 Research validity and reliability

To assure, as far as possible, the validity and credibility of the research approach, the data analysis, findings, and details concerning the research phases were documented. To ensure the internal validity of this research, Dubé and Paré's (2003) criteria for assessing case study research was applied. The criteria focus on three main cornerstones: research design, data collection, and data analysis. Table 3-5 provide an overview of the assessment.

There are several techniques for maintaining the validity and credibility of qualitative research. The technique applied in this research is triangulation of subjects. Triangulation is a technique where the researcher uses more than one method or source of evidence (Bryman 2012; Yin 2018). This research used the literature review for identifying the knowledge gaps within the use of IoT in diabetes treatment and challenges regarding patient privacy, which further aided in identifying several stakeholder groups. These data sources helped gaining understanding of the relationship between the gain from using IoT in diabetes treatment and perceived privacy challenges across the groups.

Criteria (Dubé and Paré 2003)	**Assessment comments**
Research Design	
Clear research questions	The study presented clear predefined research questions.
A priori specification of constructs and clean theoretical slate	The study used priori constructs derived from existing literature and previous research. New issues emerged from the data, which point towards the need for further research.
Theory of interest, predictions from the theory, and rival theories	The research adopted several theories about challenges related to privacy and security, and cyberthreat for IoT adoption in the healthcare sector. These theories formed predictions and assumptions that were investigated through the interviews, challenging existing literature on the benefits from IoT in patient care.
Multiple-case design	It was decided to include one case, yet several stakeholder groups were included in this research. Therefore, a single-case design was applied.
Nature of single-case Design and Replication logic in multiple-case design	The selected case was chosen based on being critical (Yin 2018).
Unit of analysis	The unit of analysis was stated as the three stakeholder groups: (1) diabetes patients, (2) healthcare personnel, and (3) industry representatives.
Pilot case	A pilot case study strategy was not used; however, the insight from the study by Cleveland and Haddara (2021) have aided the process and structure of the data collection in this study.
Context of the case study	The context of the study has been described in detail.
Team-based research and different roles of multiple investigators	Only one researcher was involved in the data analysis of this study. In an attempt to decrease bias and increase reliability, interviews were recorded to make sure no words were disregarded, and interview guides, findings, and analysis were thoroughly discussed with critical peers and master thesis supervisor.
Data Collection	
Elucidation of the data collection process	The data collection process and data sources have been described in detail. Additionally, several tables and figures are included to provide information about the data collection process. This research followed the guidelines for ethical research provided by Kristiania University College. The interview participants' personal information has been handled accordingly to comply with GDPR.
Multiple data collection methods and mix of	This study relies entirely on qualitative data. The primary data sources were interviews, conducted through video conferencing (patients and healthcare personnel), phone calls and e-mail (industry representatives), and literature review.

qualitative and quantitative data	Notes were taken during all interviews, those conducted through video conferencing were also recorded, to ensure the interpretations of the data was valid. By including three groups of stakeholders the internal validity of the findings was improved.
Data triangulation	This study has employed data triangulation by comparing the perspective of the three different stakeholder groups and existing literature (Patton 2015).
Case study protocol and case study database	Interview guides were developed and reviewed by peers and master thesis supervisor prior to conducting the interviews. These guides were used throughout the interviews, and included questions grouped according to the research topic. Additionally, all participants received information about the research and how their answers and identity would be anonymized if they decided to participate. As their interviews were scheduled to be recorded, participants in the patient and healthcare personnel stakeholder groups signed an information and consent form prior to the interview.
Data Analysis	
Elucidation of the data analysis process	An overview of the data analysis is provided in section 3.3.

Table 3-5: Internal validity assessment.

3.5 Ethical considerations

To comply with ethical research requirements, the research was conducted in accordance with Kristiania University College’s dedicated research ethics guidelines based on the overarching regulations (Kristiania University College 2022). By following these guidelines, the researcher ensures ethical treatment of the stakeholder participants.

This master’s project, to some degree, relates to the aspect of healthcare; therefore, an application seeking REK’s (Regionale komiteer for medisinsk og helsefaglig forskningsetikk) approval was initially submitted. However, REK considered the project to not be within the medical aspect of healthcare, and therefore it does not apply to the Health Research Act, and there is no need for approval from REK (REK 2022).

As the focus of this dissertation was to capture the perception of the individual patient and healthcare personnel, and these interviews were scheduled to last up to one hour, it was decided to do voice recordings during the interviews to capture all details when transcribing, minimizing the possible loss of important information. As of this, an application seeking NSD’s (Norsk senter for forskningsdata) approval for using Microsoft Teams and doing voice recordings was submitted to make sure the personal and sensitive data was managed safely and ethically. The application was approved.

All patients and healthcare personnel received information about the dissertation's ethical guidelines and signed a consent form before the interview (Appendix A). Following the principle of data minimization (Kristiania University College 2022; NSD 2022), the interviews with the industry representatives were considered not necessary to be recorded. They were scheduled to last no more than 15 minutes which was deemed to be manageable to transcribe without losing important information. Due to this, they were not included in the NSD application. All industry representatives received an e-mail describing the project and why they received the interview request (Appendix B). For confidentiality purposes, all fifteen participants were anonymized. Their identity has been replaced by letters indicating their stakeholder group and number in the order of when the interview in that group was conducted, as aforementioned. Participants could, at any time, ask to get access to their data or have it deleted. None of the participants have requested this. All personal data and interview recordings are being stored in Kristiania University College Database until the end of June 2022.

4. Findings

The objective of this study was to investigate the impact of IoT in diabetes treatment on patient life-quality and the relationship between the assumed increased life-quality and potential cyber risks related to this type of technology. Hence, the following research questions were addressed:

RQ1) How does diabetic patients experience their life-quality after changing from manual equipment to IoT-based equipment?

RQ2) How does healthcare personnel (working with diabetic patients) experience patients' life-quality after changing from manual equipment to IoT-based equipment?

RQ3) What are the stakeholders' perspective on privacy and security related issues in using IoT for treating diabetes?

4.1 Findings from patient interviews

4.1.1 Living with diabetes

Being diagnosed with diabetes is described as a life-changing event that is difficult to deal with both mentally and physical, regardless of the patient's age. Many things and routines need to be changed and taken care of to keep the glucose levels stable and prevent possible diseases related to diabetes, such as repeatedly painful needle punctures and diet changes. All patients explain they have experienced feelings of anxiety related to fluctuating glucose levels. "It was a big challenge to begin with – the insulin and glucose levels, understanding how it all adds up. Also, I was terrified of needles, I still do not like them, and the skin punctures hurt." – (P1). Three out of five patients explain the constant need for skin punctures to measure glucose levels and inject insulin were dreadful. All patients have experienced inflammations due to this and had to change where on their body they did the puncturing from time to time to avoid it. Additionally, P1 and P5 describe traumatic episodes of panic attacks due to severe anxiety of needles.

Not only is diabetes hard on the diagnosed patient; the three patients being diagnosed under the age of ten describe their parents' constant fear of their child's life and having to wake up several times a night to measure glucose levels on a terrified, screaming child as horrible and exhausting memories. "For my mom, my diabetes became a full-time job. Because it was difficult to control, she quit her job to take care of me." – (P3). The patient diagnosed as a teenager explained that her parents were worried to begin with, and as she was old enough to handle her diabetes herself, they tried to change up the diet for the whole family to assist in controlling her glucose levels. "I remember my parents starting to stress over our meals and immediately bought several cookbooks with "blood sugar friendly" recipes. They used them for a while until we realized I can eat about the same as before; I just have to be more careful and adjust my insulin." – (P2).

The three patients diagnosed as children felt embarrassed when having to do manual glucose measurements and insulin injections in public and at school growing up. As teenagers, they were self-conscious and uncomfortable when using previous insulin pumps, as their bulky size made them visible even underneath clothes, resulting in the patients sometimes removing them so that others would not notice. The patient being diagnosed as a teenager explains she never felt embarrassed or self-conscious monitoring her diabetes, but it could sometimes be problematic to inject insulin as it would require some undressing. "Even though I have not had a problem using manual equipment in public, I sometimes postponed injections and measurements because I would have to show off skin. Now I can check my levels and adjust my dosages even in rush hours standing in a crowded bus." – (P2). Three of the patients described keeping up with the measurements was difficult when using manual equipment, the other two considered it not to be difficult but a hassle. They all, however, experience the transition to CGM and newer insulin pumps has made it easier and offered great relief, as it is more seamless and automated.

4.1.2 The impact of using IoT in diabetes treatment – a patient perspective

All patients have switched from manual glucose meters and insulin pens to IoT-based CGMs and insulin pumps. Four of them have been using CGMs and pumps for several years, while one started six months ago. How the experienced starting using IoT equipment varied. Some explain their biggest hindrance before and concern when starting using diabetes technology was feeling sicker than they are and more self-conscious because they would have something visible attached to their bodies. Others experienced panic attacks due to seeing their glucose levels fluctuating on the CGM display, feeling all they did was start and stop insulin injections and eat a lot in desperate attempts to stabilize it. After a while, they got used to the equipment being attached to them and were calmed by healthcare personnel about natural glucose fluctuations. Now, all five patients explain their lives to be "as close to normal as it can get" and experience their life-quality to be "better than ever" after starting using their current equipment. "Initially, I didn't like the idea of devices and wires being attached to my body, but now I regret not having started earlier. I cannot describe how much this technology has changed my life." – (P1).

CGM was mentioned as the most revolutionizing device out of the two technologies, as glucose measurements needs to be taken more often than insulin needs to be injected. However, patients also experience a big relief using insulin pumps, as they offer automated processes, even though they are more visible than CGM. Both devices have enhanced the patients' control of their diabetes. One patient explains that before using IoT, she was negligent towards her diabetes and did not measure glucose or inject insulin as often as she should. Now, she feels more confident and competent in taking care of herself and has learned more about her diabetes. "I feel like the pump and sensor have become a part of me." – (P5). After starting using CGM, all five patients experienced their HbA1c to stabilize. Additionally, the two patients using the closed loop solutions explain that their HbA1c is *almost perfect* after using these technologies for six months. They also explain that they have not experienced worries related to hypoglycemia or hyperglycemia after starting using closed loop, as they predict and regulate insulin injections based on CGM readings. "I feel like I hardly look at my pump anymore; it is like I'm living a normal life!" – (P3). Three patients are currently using the CGMs' mobile app to read their glucose levels; the other two reads them on their insulin pumps. Thus, all patients only carry one control device for their equipment: the insulin pump itself or the pump's connected PMD.

4.1.3 The future of diabetes IoT

The patients that have used IoT for several years describe significant improvements over the years; the devices have become more seamlessly in their integrations and more reliable and durable for each update, making it easier to control their diabetes. In a long-term perspective, this can prevent other diseases related to diabetes, which will additionally lower the cost of potential treatments for the Norwegian government. "The equipment itself is more expensive than insulin pens and manual glucose meters, but long-term, it is more beneficial for the society as I'm more in control of the disease." – (P4). The patient that started using IoT six months ago cannot imagine how his equipment could become better. The other patient using closed loop sees it as beneficial if a mobile app could control the insulin injections if she would need to make manual adjustments. Additionally, she would like to have a wireless closed loop pump system, yet it would have to last longer than the three days Omnipod pumps do today as she wants to limit her skin punctures. The other three patients agree that an app to control their insulin would be helpful because they would not have to undress if using a wired pump, and they would have one less device to carry if already using a wireless pump. Both patients using Omnipod are positive to start using a closed loop system. Initially, they would like to continue using a wireless pump, but after giving the benefits a thought, one of them would consider changing to a wired pump if Omnipod's solution is not made available through the Norwegian healthcare program or gets severely delayed. One of these patients has been told by her diabetes nurse that it is scheduled to launch in Norway later this year. The patient that has not gotten her t:slim pump updated to Control IQ is aware of the update and what benefits it might offer but does not mind making some adjustments herself.

In general, the patients would prefer if the insulin pump and CGM could be combined in the same physical device so that they would only need one device attached to their body and carry fewer PMDs. They do, however, understand there are challenges related to the placement of the sensor in relation to the insulin syringe. Additionally, two patients mention artificial pancreas as the ultimate improvement of their life-quality. Still, they do not see that as an option anytime soon due to the excessive need for testing to ensure it is safe. One of these patients suggests the CGMs and insulin pumps could be smaller in size, as they still feel bulky underneath clothes. Four patients mentioned it would reduce the number of skin punctures and benefit the environment if the equipment would last longer than three to ten days.

Lastly, all five patients see the advantage of the data their equipment generates to be used more actively in their treatment and would like it to automatically be transferred to a diabetes management system for healthcare personnel to access even without their presence. Four patients explain they are aware that by using a cable, they can upload the data from their devices to a system used at their healthcare institution. Still, they only do this if healthcare personnel explicitly request it, as they describe it as difficult and time-consuming to get the connection between the device and system to work. "It would be nice if they could use the data for something, but it needs to be transferred regularly without me having to do anything." – (P3).

4.1.4 Privacy, security, and safety concerns – a patient perspective

When asked about how they view their safety using IoT, four out of the five patients stated they are not concerned at all. They trust that the pump will deliver the correct insulin injections and that the CGM readings are reliable. "I may be naive, but I utterly trust this technology." – (P1) and (P5). One patient admits the thought of the pump injecting more insulin than what is instructed, or someone hacking the pump and injecting the full reservoir have slipped her mind. She is, however, convinced she would notice before it would be injected as the syringe is too small to process the whole reservoir at once. All five patients' initial response was that they would have just removed the pump if they experienced any abnormalities with their glucose levels to stop the insulin injection. Two patients got to thinking that if they did not notice, they would be in a more critical situation. "There is a limit for how many units can be injected in one session, but as far as I know, there is no limit for how many sessions you can perform repeatedly. If my glucose level were four and someone injected 20 units, it would be a big issue. If they injected the whole storage, 200 units, I would probably die." – (P3). Another patient got to thinking about an experience where her PMD broke down and expressed minor worries about a repeated incident. Yet, she explains she would just order a new one and use insulin pens for a few days until she got it. If the pump was controlled by an app, however, she would be more worried about always having her phone fully charged.

When asked about data privacy, four out of the five patients admit they have not given their privacy and security related to their equipment any thoughts. One has been made more aware of privacy challenges and cyberthreats over the last couple of years yet has not offered her own privacy any additional thoughts. In regards of potential cyberthreats, four out of five patients are not at all worried about their equipment being hacked, one sees it as a potential, yet unlikely, risk. They all consider their phone being stolen as a bigger risk, yet they do not think anyone would be interested in the diabetes apps. None of the patients considers their diabetes data to be sensitive information or of interest to others than their healthcare personnel, and therefor the risk of someone hacking their devices and leaking their information as low. In these terms they all consider Norwegian privacy regulations to too strict, as they do not mind their healthcare institutions accessing their data remote prior to their appointment to provide better treatment and reduce physical visits for regular check ins where there is no need for medical examinations.

Patients are not sure what data (except glucose measurements and insulin injections) is registered about them, how it is stored, and who has access to it, but at the same time express they do not care. None of the patients have read the privacy terms and conditions for their equipment and software. One made a guess the data is stored in the cloud and is only accessible for their diabetes nurse and doctor. When checking their devices and apps, two patients found that limited personal information (name, phone number and e-mail address) and some manually added glucose measurements were stored. Another patient found more sensitive information (personal ID, a picture of herself, height and weight, and year of diagnosis) in addition to some automatically uploaded glucose measurements being stored. Yet, even after these reveals, the patients do not worry about their privacy. Three patients explain they probably would be more worried that the data could be used against them, to not get a job or insurance, if living in the US. One of them adds that if she was being discriminated in a job interview process or at work based on having diabetes, she would not have any interest of working for that company. When giving it a thought, one of the patients express she is a bit critical towards how her information is handled, as she has experienced information being sent to the wrong address. "If they don't have control of something so simple as my address, when I've informed about my new address and they have confirmed the change in their system, should I be trusting them with my medical data? For example, they send pictures and information about my eyes to another hospital to run diagnostics, what if that is lost in the mail? Or other, more sensitive information from my journal? I don't really know how they share patient information or handle my data when I think about it?" – (P3).

Three out of five patients mention their lack of worries in data privacy and cybersecurity can be related to ignorance and not having been exposed to breaches. One patient is aware of potential cyberthreats and is to somewhat degree worried about hacking, yet more so of her phone being hacked and images and messages to be leaked than her diabetes equipment being the target for the attack. Only one patient sees the potential danger if someone were to use their equipment as an entry point for hacking other, larger systems, but at the same time considers the risk for this to happen as low. "By using apps and cloud-based technology my phone creates a new entry point for hackers to access other information and critical systems that is beyond what revolves me. But what's the chance of that happening in Norway?" – (P3). Four out of five patients admit to slack on best practice for passwords and security precautions in general; they use weak passwords, re-uses passwords, and sometimes does not use passwords for their devices and accounts. They explain reasons for this is having a bad memory and ignorance as they have not been a victim of hacking. One patient selectively uses 2FA for the accounts she considers most important. Another uses it whenever it is offered, but also admits to re-using passwords. None of the patients updates their passwords unless they are explicit asked by the device or system to do so, have forgotten their password, or discover log-in attempts from other locations. Patients express they probably would be more conscious towards password security if insulin infusions were controlled by an app. Yet, some describe it would be annoying if they had to enter a code every time they would adjust the insulin, as it already is annoying pressing the keys on the PMD or pump in a specific order to do this today and would rather prefer biometric identification. After giving password security a thought, three patients wonder why their CGM app does not require a personal password or biometric identification for entering, especially for uploading glucose measurements to other systems. "It would be more annoying, but at the same time it would be safer." – (P5). Additionally, one patient raised her concern for a potential app that controls the insulin pump to make sure the app version is compatible with the iOS-updates. "Today, the Dexcom app is warning me to do iOS-updates unless I have controlled the update and current app version is compatible. I have ignored the warnings until now, but I would probably be more careful if it was related to the pump as that is more critical." – (P4).

In general, patients' level of worries related to privacy and cyberthreats are low and find the Norwegian regulations in terms of how their diabetes data can be utilized to be too strict, but at the same time they feel safe. They consider the gain from using IoT for treating their diabetes as more rewarding than the potential harm caused by cyberattacks.

4.2 Findings from healthcare personnel interviews

4.2.1 The impact of using IoT in diabetes treatment – a healthcare personnel perspective

Healthcare personnel (HCP) describe diabetes as a time-consuming disease. It requires a lot of planning, and it is difficult to perfect insulin dosages, even by using modern technology. As diabetes is an individual disease, all patients have different challenges and experiences dealing with it; the technology and treatment that works for one patient might not work for another. This makes it challenging for HCP to always provide high quality treatment. They do, however, explain that CGMs and insulin pumps often offer great assistance and tools both for HCP to provide better care and for patients to monitor their own diabetes. However, some patients use a long time deciding to try it out. According to HCP, the most common reason for patients being hesitant is that they fear it will make them feel more limited and sicker than they are, as the devices and wires would be attached to their body and visible to others. After the patients have used the equipment for some time, HCP see a pedagogical effect, as the patients realize they should be more aware of how their glucose levels are affected by different types of food and insulin dosages. They also experience patients feeling an increased life-quality from using

IoT, especially the new closed loop solutions; patients upgrading to closed loop have drastically improved their average daily glucose levels in range in just days and HbA1c in months. "It's inspiring to work with diabetes technology when you see results like that." – (HCP1).

There is some disagreement among HCP when it comes to revolutions within diabetes treatment. Four out of five HCP consider the new closed loop solutions and the newer, more stable, and smaller CGMs as revolutions, as it delivers the most accurate measurements and is what closes resemble functioning pancreas. Despite patients feeling their life-quality is improved, one doctor explains: "There has not been a *revolution*, there has been gradually *improvements* in the technological equipment for sure, but according to the diabetes registry, there is no significant change in the average HbA1c, hypoglycemia or hyperglycemia cases over the recent years. It's still challenging as the wrong volume of insulin is injected to the wrong time at the wrong place of the body. However, patients using IoT express a big relief and impact on their life." – (HCP2). The other doctor and two nurses, on the other hand, explain they see an improvement in the HbA1c for patients using closed loop solutions, and therefore recommend most patients to try it. However, the closed loop solutions require extra appointments with each patient to provide additionally information and make sure the patient are suited for handling that specific technology.

Due to the increased use of diabetes technology, HCP explain they give treatment and advice of higher quality than before as they get a better overview and insight to the patients' everyday life with the data available from their CGMs and insulin pumps. It gives a better foundation for making treatment plans and visually explain each individual patient's diabetes. However, the nurses explain it is more time-consuming with patients using IoT, as it takes time to connect to patient devices, load data and dashboards, and technical error sometimes occurs. Due to privacy regulations, they also must read and interpret the information, find the correct treatment, and adjust the treatment plan with the patient present. Both nurses and doctors express this as frustrating and explain it to be inefficient.

4.2.2 The challenges of IoT in diabetes treatment

The nurses describe they experience challenges with downloading patient data, it does not always work and takes a lot of time to restart both software and hardware. This must be done with the patient present as they cannot access the data remote or prior to the appointment. All HCP agree patients using IoT are more resource consuming. It requires a lot of time to inform the patients about the technology and training them in how to use it; how it works, how it could work, what happens if they do not use it correctly or frequently enough, how to handle different scenarios, and be sure the patients fully understand before they start using it. Potential errors and how to handle them is one of the main challenges for diabetic patients, in addition to re-learning key functionality for software updates and new devices. All HCP consider information to be the most crucial part of diabetes technology; both the information they give patients and how they follow up patients using it, and to be informed themselves and keep up to date. They find it challenging to stay on top of it, as the development of new technology is expanding, and the marketing of medical equipment has become more aggressive over the years. Further, they all explain there is a lot of functionality in the current technology that is hardly being used that could and should be utilized before patients upgrades to newer technology. The problem is that they do not have the time or resources to train the patients in all functionalities, which results in patients struggling to use the technology efficient, have a hard time finding the information HCP requests, and not understanding all the parameters in the PMD display. “Most often we start out teaching the patients the basic and crucial functionality with the intention of building on it at a later point, but as we lack time and resources, we cannot prioritize further training.” – (HCP3). Additionally, they experience most patients always want the newest equipment and latest updates immediately, despite having fully functioning devices or not needing all functionality. “If they would have continued with their equipment for a while longer – it most often still works without errors, it is just not the newest and hottest version, they could learn how to use it more efficient and possibly experience more benefits and improvements.” – (HCP2).

One of the nurses suggest an enhancement for insulin pumps would be an app to control insulin injections, as it would be more efficient and accessible to do adjustments. This would especially make an impact for patients with wired pumps using clothing, such as dresses and religious clothing, which makes it unpractical for adjusting insulin in public. Another nurse considers the current equipment as unpractical with all the different components and would consider a pump and CGM combined and smaller in size more practical. She also explains there is excessive packaging, which does not contribute to sustainability; big boxes with lots of air and components carefully packed in each their own disposable plastic case even though they must be put together to work. Four out of the five HCP express accessing and utilizing patient IoT data real-time remote would make their job much easier, more efficient, and allow for them to provide even better, more qualified, and personalized treatment and patient care. “It would be a great resource if the IoT data could be transferred automatically to the patients’ journal and be used in combination with the clinical data.”- (HCP2). They further explain the possibility for accessing real-time and historical data is there, as they know other institutions in other healthcare regions that use this. One HCP suggested the different healthcare regions in Norway are following different guidelines for privacy when it comes to how this data is utilized in treatment. As all HCP in this study works within the same institution, and therefore the same healtcareh region, they follow the same guidelines and are not allowed to access and automatically transfer data from patients' insulin pump and CGMs to their journals – even if the patients gave their consent. "I see a great advantage in accessing real-time glucose levels for healthcare personnel, patients do not tend to care much about their diabetes data anyway." – (HCP4).

4.2.3 Privacy, security, and safety concerns – a healthcare personnel perspective

In general, HCP trust the medical companies, and experience them to be very conscious about safety and privacy as breaches can result in lawsuits and sees this as somewhat an extra insurance for the equipment. They also explain that the medical companies have stated it is impossible to hack their devices. HCP experience most patients are not concerned about this, or care to read the terms, conditions, and privacy agreements, when using IoT equipment. "If they do it accept the privacy terms, they are not able to use the technology that most likely would ease their troubles and improve their life-quality, they are left no choice but to accept whatever is written in the conditions." – (HCP4). Additionally, they experience patients to not consider their diabetes data to be sensitive, and that many understand the value of their data being shared with the healthcare institution, and therefore would like for HCP to access it remote for treatment related reasons. Further, two nurses explain patients sometimes are being frustrated by the privacy regulations being too strict, as they just want help to manage their diabetes in the most efficient way. Four HCP think patients should be a bit more critical towards how technology generate, store, and share data, but also how their data is managed at healthcare institutions. One nurse explain she is a bit concerned about what data is shared with manufacturers and is curious to why patients are not more critical. Additionally, one doctor considers the discussion about who owns the data to be very important and is worried about manufacturers potentially owning patient data. When asked about their own opinion about the sensitivity of diabetes data, all HCP explained they find diabetes data to be sensitive information but consider other medical data to be more delicate and find the privacy regulations in their healthcare region regarding diabetes data to not be very functional for working digital. "Security in regards of privacy is extremely strict within the institution and healthcare region – almost too strict. We can't take full advantage of the diabetes technology due to this. If these systems were placed in the cloud and we access them by using BankID or some equivalent 2FA

I think it would be safe for both patient and systems.” – (HCP5). Additionally, HCP suggest it should be up to each individual patient to make their own decision about their data being shared it with healthcare personnel.

Four out of five HCP are aware of cyberthreats towards the healthcare industry. In case of an incident where an insulin pump is hacked, they explain the hacker would have to know exactly which buttons to press in which order to interfere with the insulin injection. One HCP consider it as unfortunate if diabetes equipment and apps are hacked, but only as they are useful for patients and is not concerned about privacy or security being compromised. She explains she cannot see how leaked diabetes information can harm the patient or why anyone would want to target such equipment. She further elaborates that she considers smartphones in general getting hacked a bigger threat than diabetes IoT and apps. The other four consider cyberattacks as critical, yet that information being leaked as worse than equipment settings being override. They also consider the risk of cyberattacks targeting diabetes IoT as low. One nurse further explains she considers hacking of insulin pumps as catastrophically but is more concerned about cyberattacks against other IT systems and medical information and does not see how insulin pumps and CGMs can be a gateway for cybercriminals to enter other IT systems. When asked if they have experienced cyberattacks, all healthcare personnel explain they have received spam and phishing emails and are instructed to delete these and report them to IT-staff, two mentions the attack against Helse Sør-Øst. One of the doctors explain she does not think the Norwegian healthcare sector have sufficient security systems, and considers this should be a priority, yet it should not compromise efficient treatment. In general, HCP consider the potential increased life-quality worth the potential risk of cyberattacks, as they consider the risk to be low, yet they feel a responsibility to ensure patient safety at their end. "Diabetes patient have enough to think about living with and managing their diabetes, they should not have to be concerned about their equipment being hacked and information being stolen – that should be out responsibility.” – (HCP4). She further explains she consider it would be more challenging to ensure patient safety if insulin injections were controlled by an app, both because there are more applications and systems in a phone that might be of interest for cybercriminals to perform an attack, and people generally can be sloppy and lose their phone or having it stolen. Three HCP mention there should be another personal authentication mechanism, such as password or biometrics, for entering the diabetes apps, and stress this would especially be important if apps for controlling insulin injections are launched.

Healthcare personnel consider their institution take patient privacy extremely seriously. All employees are required to participate in an annual e-learning course about privacy and security, yet, the institution's privacy and security guidelines does not provide a best practice guide for passwords, like how to create a sufficient password or how often they should be changed. However, HCP are aware of that they should not share their passwords. Yet, the nurses explain that all nurses in their department share one account for some diabetes management software, meaning they all share the same login information. For entering other systems, such as the patient journals, they use individual accounts, and all activity is traceable. "Who enters and the activity in a journal is recorded, but if someone steal my ID and do harmful actions it would look like it was me, that would be horrible! I am, however, not afraid of this happening, and that might be because I have not heard about anyone experiencing it." – (HCP2). They further explain that some systems require 2FA, such as BankID, others just an ID and personal password. Four HCP explain they use 2FA when available, even if it is not required. One admits to allowing "remember this device"-function for staying logged in when available, another admits to re-using passwords and not having as complex passwords as they might should. The HCP disagree how often passwords are changed; two claim the passwords for their shared users is hardly ever changed, while one claim it must be changed every 90 days. Some claim the systems with individual accounts force password changes at regular intervals, while others explain it is up to each individual employee to create passwords and update them.

4.3 Findings from industry representative interviews

4.3.1 Cyberthreats in the healthcare sector

The cyberthreat level is described as similar across all sectors: evenly increasing over the recent years, with a simultaneously increased security focus. During the Covid-19 pandemic the healthcare industry experienced becoming an even more lucrative target for cyberattacks. "One explanation could be that the attackers see the healthcare sector being in a highly pressured situation and thinks they are more likely to pay ransom to get out of the situation" – (IR1). Industry representatives explain it has not been reported in Norway yet, but there is an increasing trend internationally. According to one government representative, there has only been two successful cyberattacks against the Norwegian healthcare sector: Helse Sør-Øst in 2018 and Østre-Toten in 2021. He further explains it is expected that there will be more targeted attacks like this in the future.

Industry representatives agree there used to be a lack of sufficiently secured medical equipment, but that cybersecurity in the healthcare sector has been strengthened over the last years. Now, manufacturers are more aware, and work targeted with security to ensure patient safety. One of the company representatives explain they have been highly aware of the surrounding cyberthreats and hiring dedicated people to ensure they uphold premium security levels. Due to recent events in Eastern Europe, they have even increased this focus. “As some of our products are distributed in Russia, we are now listed as a potential cyber target for Anonymous [hacker activists]. Due to this, our safety precautions have been increased further. It would be a disaster first and foremost for our patients if this attack becomes a reality – if their medical data gets leaked or their equipment stop working, but at the same time it is one of the risks when using technology.” – (IR3). Both company representatives claim their equipment have never been exposed to cyberattacks, security breaches, or data leaks, both on a national and international level. One of them states that the only way of getting a hold of data from their diabetes equipment is through their own software or Diasend, and that the devices only communicates through Bluetooth with the corresponding insulin pump, CGM or CGM app. Additionally, each device has a unique ID and code that ensure data is collected from the correct source. None of the industry representatives consider diabetes IoT to be in greater risk of being a target for cyberattacks than other medical technology. In terms of danger, one industry representative states that attacks that target pacemakers would possibly be more critical and life-threatening than those targeting CGMs or insulin pumps, as the CGMs cannot *do* anything, and the insulin pump can be removed. Yet, she considers it as extremely unfortunate if diabetes equipment is attacked, considering the trouble associated with living with diabetes. This is supported by another industry representative, which adds that patient data need to be protected at all costs. When asked if an attack against the app or the PMD could be a gateway for entering larger databases and systems, they explain that all equipment and technology is security certified and has been evaluated across Europe before being approved for the Norwegian market, and therefore is safe for patients. Additionally, all industry representatives consider the data generated by the diabetes equipment itself not to be of interest for others than the patient and their healthcare institution, and therefore does not consider it a risk being leaked. They do, however, point out the need for security in these technologies, as it is personal data, and many patients depend on the equipment and technologies to work.

4.3.2 Privacy, security, and safety concerns – an industry perspective

According to the industry representatives, privacy regulations most often get the blame if new diabetes technology is not released in Norway, while the problem often is about practical implications in implementation. All medical technologies must be risk and privacy assessed before Norwegian patients can start using it and this process is time and resource consuming.

The industry representatives pose this as a dilemma as at one side technology must be safe and someone must be responsible for ensuring safety, but at the other patients seem not to care that much about their own privacy and security; they just want to start using technology they believe will help their situation. When asked if Norwegian privacy regulations are too strict when it comes to diabetes data, one government representative explain this is a new issue that is yet to be discussed and evaluated. He further explains there lies complex, juridic questions within the scenario of patients wanting to decide for themselves if their data is shared with their healthcare institution. "Traditionally, insulin pumps are something that has been managed and provided to the patient by the hospital, but with the new technology new opportunities is revealed. Providers offer technology such as CGMs which allow for patients to access their own measurements, and it poses a question as to who is responsible for patient safety. There is a complexity there, and it is not necessarily about if privacy regulations are too strict, but who owns the data the technology generate." – (IR1). He is supported by the legal advisor, who adds that what should be discussed and investigated further is how and what type of data is captured, handled, and transferred. He further explains some of the companies are using as much as 150 cookies in their apps and websites where diabetes software is accessed, which are considered unnecessary even for analytics and marketing. By reviewing the privacy of diabetes equipment in the Scandinavian market, he experiences the transparency among the different providers varies, which poses a challenge for users of this technology. He adds that some of the companies are more cooperative and reply more quickly than others in terms of providing requested information about the aspects of data handling, data integration, and patient privacy when it comes to diabetes devices and corresponding apps, software, and analytics. He explains they might not intend to keep it a secret, that in many cases this is companies that traditionally has been providing hardware and equipment managed on premise by the healthcare institution and now suddenly are developing apps and analytic software that both patients and healthcare personnel are able to access remote. Adding this is still a new issue, where these companies are learning how to provide what the market wants, and there often is a lack of knowledge within these companies towards how privacy should be handled and how the local privacy laws when expanding outside their country of origin. Further, he describes considerable variations in the different policies assessed, and that it is unclear how many parties are involved with and who is responsible for the data. This poses a possible ethical challenge in terms of healthcare personnel and institutions being able to recommend different diabetes equipment if the data is used for triangulation. Medical equipment providers often cooperate with other companies for analytical, research or technical support purposes, including several participants to be involved with patient data, yet this part is not described thoroughly in most privacy policies. This is challenging, as many of the diabetes technology providers are based in the US, use American hosted cloud services for handling data, and cooperate with other US based companies, leaving data to be transferred to a third country, which calls for the Schrems II judgement to be addressed. He further explains he does not consider cloud services to be a problem, rather a solution. But for diabetes technology to be secure and functional for the patients, companies must be organized and structured when it comes to privacy and ensure patient information and medical data is handled in a sensible, reasonable, and secure way. "From my point of view, the three main challenges within healthcare and diabetes IoT are (1) the providers' privacy transparency, (2) the different parties' use of cookie and further what the data collected is used for, and (3) the possible transfer of data to a third country." – (IR4).

One government representative experience that the bigger the healthcare institution is, the more resources are located to actively work with information security, privacy and GDPR. He further explains that the large institutions are also at greater risk of experiencing targeted attacks, while the smaller institutions might be at bigger risk of being hit with by random attacks. When asked if how healthcare personnel handle medical data today is sufficient to uphold good privacy and security, he explains that big institutions have systematic training for information security, while smaller institutions lack this. The Norwegian government is currently working on a strategy for digital security in the healthcare sector, where measures that are being evaluated includes a common competence development for smaller institutions. But as of today, patient data security much depends on the individual personnel. One company representative express she does not think the cybersecurity in the Norwegian healthcare sector is sufficient and does not think that moving all patient information to one single national cloud service is the answer. Both representatives from the government and the companies explain they have objectives for a more digital healthcare sector, both regarding systems used in the institutions, equipment provided to assist patients, how information is structured, stored and secured, and how these components communicate. Due to these objectives, the industry representatives in general explain they expect the discussion regarding privacy and security in the healthcare sector to keep growing, and sees this discussion as positive, important and about time. One representative further explain that the current privacy landscape is unclear and complex, causing confusion regarding equipment. "Even though we are providing information about privacy and are following GDPR, healthcare personnel feel insecure and often need assistance to make decisions when working with technology." – (IR3).

Further, there is some disagreement about who owns the data collected from insulin pumps and CGMs. One claim it is owned by the patient whose measurements are registered, another that it is owned by the healthcare institution as the data becomes a part of a journal which they are responsible for keeping secured. Some representatives express their concerns about the technology developers getting the ownership of patient data in return of patients using the technology. One company representative claim that only patients and healthcare institutions can access the data. None of the industry representatives experience patients to be critical about their own privacy and security. One government representative considers that patients cannot do much to ensure their own cybersecurity other than trust that the information is secured, but also encourage them to ask questions about how their medical information is stored and secured and be more actively aware. Further, all industry representatives explain they experience some healthcare personnel to be a bit more critical but perceive the majority consider that if equipment and technology is approved it is safe to use. One industry representative adds that some healthcare personnel have become more aware and critical after the Schrems II judgement recently, as some diabetes equipment uses American cloud service providers. For ensuring patient safety, one industry representative considers individual competence among healthcare personnel to matter when it comes to digital services in the healthcare sector, and that healthcare institutions should aim to uphold good technology hygiene. One company representative experience those deciding which equipment and technology to be provided by the Norwegian government to be very interested in and evaluating how data is generated, stored and who has access to it. Nevertheless, three out of five industry representatives regard the discussion about data ownership and data handling consent a pressing and legal dilemma that needs to be addressed and discussed thoroughly.

4.4 Summary of the findings

Table 4-1 presents a summary of the main findings of this study, which is divided into five themes on the left column with the findings from each case in the three right columns. These themes are further used in the discussion to answer the research questions.

Themes	Patients	Healthcare personnel	Industry representatives
The impact of diabetes IoT	• Increased life-quality • More in control of their diabetes • Improved HbA1c • Reduces complications	• Increased patient life-quality • Increased quality patient care • Pedagogical effect • Reduces complications	

The future of diabetes IoT	• Control insulin injections with an app • Longer lasting, smaller, and combined wearables • Combine IoT data with clinical data, automatic transfer	• Combine IoT data with clinical data, automatic transfer • Utilize current technology's functionality • Longer lasting, smaller, and combined wearables	
The challenges of diabetes IoT	• Several devices	• Time-consuming	• New complex, juridic issue about data ownership and sharing
Privacy and security related to diabetes IoT/healthcare	• Ignorant towards privacy • Trust the manufacturers to have sufficient security • Unaware of what data is stored and how it's used • Does not consider diabetes data as especially sensitive • Negligent and selective security routines • Too strict privacy regulations	• Aware of privacy issues • Trust the manufacturers to have sufficient security • The discussion about data ownership • Does not consider diabetes data as especially sensitive • Find privacy regulations to be limiting • Different practices across the country • Participate in annual e-learning • Negligent and selective security routines	• Increasing awareness within the sector • Manufacturers work targeted with privacy and security • The discussion about data ownership • Issues regarding data handling and associated parties • Lack of transparency in privacy policies • Unclear landscape
Cyberthreats related to diabetes IoT/healthcare	• Unaware of cyberthreats • Consider it low risk	• Aware of some cyberthreats • More concerned about other IT systems than IoT • Consider it low risk	• Increasing cyberthreat level • Diabetes IoT is not more exposed than other medical IoT

Table 4-1: Summary of findings.

5. Discussion

As presented in the literature review and findings, the great potential of IoT in diabetes treatment is followed by various challenged factors within privacy and security which is further discussed in this chapter. In order to answer the research questions, the discussion has been divided into two main sections: 5.1 The impact and challenges of diabetes IoT and 5.2 The privacy, security, and safety concerns with diabetes IoT.

5.1 The impact and challenges of diabetes IoT

Diabetes is described as a challenging disease, both by patients and healthcare personnel. Previous research (Cleveland and Haddara 2021; Longva and Haddara 2019; Saltzstein 2020) described how IoT in diabetes treatment potentially can improve diabetic patients' life-quality. In this study, patients confirm their life-quality has been drastically improved, explaining their lives to be "as close to normal as it can get" and experiencing their life-quality to be "better than ever" after starting using their current equipment. For instance, the two patients using closed loop technology feel like they do not have diabetes anymore. Similar observations are registered by healthcare personnel, that additionally express they find it rewarding working with IoT in patient care as it offers a richer ground for decision making which enhances the quality in patient care. This further aligns with other research explaining IoTs ability to provide real-time patient monitoring without interfering with the patient's life has transformed patient care (Abdollahi, Moghaddam, and Parvar 2019; Gómez, Oviedo, and Zhuma 2016; Islam et al. 2015; Kintzlinger and Nissim 2019; Patil and Seshadri 2014; Rehman, Naz, and Razzak 2021). However, the use of IoT was also found to time-consuming for healthcare personnel, as there is a constant stream information that needs to be read and communicated, both in terms of product and software updates and releases, and IoT data of several months must be interpreted during the scheduled patient appointment to develop a treatment plan.

Both patients and healthcare personnel described that the use of IoT has a pedagogical effect, as patients become more aware of what affects their glucose levels by the visual pointers displayed on the PDM screens, leaving patients to feel more in control of their own diabetes. When patients are in control of their diabetes, they reduce the potential complications related to diabetes. Further, all patients and four out of five healthcare personnel explain the HbA1c has been significantly improved by using CGMs. These findings correlates with the research of Britton and Britton-Colonnese (2017) and Longva and Haddara (2019) that found the use of CGM to reduce long-term complications up to 70% and reduce glucose levels by an average of 2 points. However, one diabetes doctor claim there has been a gradually improvement over the last 20 years, yet no significant change in the average HbA1c in the later years using CGM.

Further, this study confirmed that CGMs and insulin pumps has offered great relief over the years, and the integration of devices and software has become more seamless (Cleveland and Haddara 2021; Gómez, Oviedo, and Zhuma 2016). Yet, to enhance the relief even further, patients would want the equipment to become smaller, preferably combine the two in the same device, and for the wearables to last longer. They argue this would not only make the disease less visible by smaller size and fewer devices attached and carried with, but also reduce the number of skin punctures. Also, an app for controlling insulin injections was also discussed by patients and one diabetes nurse, as there would be one less device to carry and those using wired pumps would not have to partially undress to access it. However, they express such an app must require some access control opposed to the monitoring apps currently available for CGM, as the functionality is more crucial.

Similar to previous literature, this study implies that automatic data uploads from CGMs and insulin pumps to diabetes management systems, combining wearable IoT data with clinical data is the next big thing that would transform diabetes treatment. As a lot of time is lost to things that could have been prepared in advance of an appointment if patient data were automatically uploaded, remote data sharing is expressed as a desired solution, both by patients and healthcare personnel. Combined with the power of AI and Big Data, it is expected to assist healthcare personnel in an even more meaningful matter and making their job more efficient which could be crucial for patient care (Bide and Padalkar 2020; Patil and Seshadri 2014; Rehman, Naz, and Razzak 2021). There already lies great potential within the existing IoT for optimizing patient care even further. Data from all CGMs and insulin pumps can be uploaded to diabetes management systems and accessed by healthcare personnel. According to the healthcare personnel participating in this study, they are not allowed to take these features into use due to privacy regulations. However, other healthcare regions are already using these features, suggesting the privacy interpretation and guidelines different between the regions despite being the same country.

5.2 The privacy, security, and safety concerns with diabetes IoT

In general, both patients and healthcare personnel trust that equipment and technology approved for the Norwegian market is secured and consider the increased life-quality from diabetes IoT as worth the risk of cyberthreats. However, cyberthreats are increasing across all sectors over recent years, with the healthcare sector being of higher interest during the pandemic, suggesting hackers sees the pressured situation and expect the healthcare sector to give in for ransom to get out of the situation. Due to the increased threat level, findings suggest the focus and awareness throughout the healthcare sector has increased simultaneously, as providers of diabetes IoT have been working targeted with ensuring privacy and security. Yet, for diabetes technology to be secure and functional, the medical companies and healthcare institutions must be organized and structured when it comes to privacy and security. Findings indicate there is not much a patient can do to ensure their own privacy, other than ask questions, be critical, and ensure personal security hygiene, as their safety to much degree depends on individual healthcare personnel knowledge and healthcare institution routines, enhancing the statement by The Norwegian National Security Authority (NMS): leaders in Norwegian healthcare institutions should facilitate for strengthening the institution’s cybersecurity and enhance employee competence (Nasjonal Sikkerhetsmyndighet 2022):. Diabetes doctors and industry representatives expressed they do not believe the Norwegian healthcare sector is sufficient secured against cyberattacks. The Norwegian government is currently working on a digital strategy for increasing cyber competence in all healthcare institutions. As both the government and private companies have objectives for making the healthcare sector more digital, they expect the discussion about patient privacy and security to keep growing. This is believed to have a positive and important impact.

The findings from stakeholder interviews suggest diabetes IoT not to be in greater risk of cyberattacks than other medical IoT, which is contrasting the findings by (Kintzlinger and Nissim 2019) arguing insulin pumps, due to its wide range of functionality and integrations, are the most exposed PMD. One company representative explained attacks against CGMs and insulin pumps not to be as dangerous, as CGMs only display values and insulin pumps can be removed. However, as described by Alaba et al. (2017), Kintzlinger and Nissim (2019) and The Office of the Auditor General (Riksrevisjonen 2020), attack against diabetes IoT can cause data manipulation leading CGMs to display wrong measurements for the patient to take action based on, and insulin dose change interfering with injections, which threatens patients' safety and life. This study confirm the findings of (Cleveland and Haddara 2021), as patients are not concerned about hacking. While they explain they expect to notice if there were something wrong with the insulin injections and would remove the pump, they also express they would be in a critical situation if they noticed too late. Further, patients and healthcare personnel consider the risk of IoT related to diabetes being exposed for cyberthreats as low. However, both industry representatives and healthcare personnel agree there is a need for strengthened security in such equipment and technologies as patients' health rely on them to work. Previous research claims the leading factor for cyber behavior to be personal experience (Alvarez, Baller, and Walton 2021; Cleveland and Haddara 2021). The current study's findings confirm this, as patients in general are ignorant towards privacy and security and unaware of potential cyberthreats, which might be because they have not experienced any cyberattacks before. They trust that the IoT is sufficient secured by the manufacturer and that the healthcare institutions are protecting their information, and just want the technology to enhance their lives. This observation of patients is also described by healthcare personnel and industry representatives, that recommend, even though they perceive there is no major current threats, patients to be a bit more critical and ask more questions to how their data is handled. They suggest the focus on patient security could be further strengthened if patients showed more interest or criticism. Healthcare personnel, however, share the same pattern as patients; none have experienced cyberthreats up close and are generally not concerned about patient privacy or security, yet they are to some degree aware of potential cyberthreats. However, they are more concerned about IT systems containing more patients' information being attacked, than individual patient's IoT, and they do not see how IoT devices can be used as an access point for entering other systems.

The current study's findings indicate that neither patients, healthcare personnel, nor industry representatives consider diabetes data to be particularly sensitive and not useful or interesting to others than the patients and their healthcare institution. It is unclear to patients what data about them is registered or how it is handled with the use of IoT devices, correlating with the legal representative experience of companies not being transparent with their privacy agreements and data governing protocols. Additionally, the excessive use of cookies in apps, software, and websites offers skepticism towards what data is collected and how it is used, and why they are not transparent in this. There are some challenges regarding how data is being transferred and stored, as many of these companies are based in the US, calling for the Schrems II judgement to be addressed. Findings further indicate that the landscape of privacy is complex and unclear. The industry experience insecurity among healthcare personnel related to patient privacy when dealing with IoT. When lacking competence, it is difficult to understand what is allowed and not when it comes to medical technology, causing difficulties to make and delays decision making. Additionally, healthcare personnel explain the current privacy regulations act as a hindrance for them utilizing the available technology and working digital. Both patients and healthcare personnel want to take advantage of the opportunities IoT offers, by remote sharing data from the IoT to diabetes management systems at the healthcare institutions. They further explain other institutions in other healthcare regions are already doing so, suggesting institutions in different healthcare regions have different ways of interpreting and following the privacy regulations, and express they see a huge advantage in this data sharing. However, as mentioned by some industry representatives, this is a complex and legal issue that goes beyond what patients approve and do not approve for their data. Findings indicate the ownership of data generated by diabetes technology is unclear, aligning with the research by Alvarez, Baller, and Walton (2021) that further states the discussion of who owns the data generated from healthcare IoT is of imminent concern, suggesting healthcare government and medical companies should be prepared for the debate on who owns the data to be accelerated. As the healthcare regions seem to have different guidelines for following Norwegian privacy regulations, patients moving to or otherwise transferring to another region might experience a change in patient care and their treatment plan that could cause confusion and frustration. For instance, patients moving from a "strict" region to a "looser" might experience "better" care, if they want to share data. Yet, they might be more exposed to cyberthreats. Patients moving the other way might experience frustration, as they are used to being able to share their data and getting the benefits that follows. Yet, these patients' privacy and security might be safer in case of a cyberattack. According to Norwegian law, all Norwegian citizens have equally rights to access and receive healthcare services of good quality (Pasient- og brukerrettighetsloven – pbrl, 31.03.2022). Based on the findings of this study, it could be argued that the difference in how the healthcare regions utilize the diabetes technology and software can make a difference in the quality of patient care. Healthcare regions that have more limitations in how they can use these technologies does not necessarily offer *bad* patient care, but as suggested by all stakeholder groups, there lies a great value in utilizing the technology and combine the data generated by IoT with clinical data, which could provide *better* patient care.

Thus, this study addresses the need for clearing up confusion. One way would be making privacy guidelines understandable for those that does not have privacy and GDPR as their field of expertise within the healthcare sector. Providing clarity to the whole healthcare sector about who is the rightful owner of the data generated and guidelines how the data can and should be handled, stored, and secured, could contribute to unison understanding across the healthcare regions that could lead to patients all over Norway getting the same advantage of the technologies related to their IoT. Additionally, it could help increase competence among healthcare personnel to enlighten their patients, which could further lead to higher cybersecurity awareness among patients. By standardizing how data generated by medical equipment, such as CGMs and insulin pumps, can be shared by patients with healthcare institutions for all healthcare regions such differences can be avoided. It does, however, require that patient privacy is prioritized and kept safe. As one diabetes doctor argues, other cloud-based systems containing sensitive information (such as Helsenorge and banking) requires identification through BankID to be accessed, suggesting that diabetes technology could be kept safe with the same type of identification. Existing literature also suggest most Norwegian institutions would strengthen their cybersecurity by implementing ISO/IEC27001 (Kjærnli 2021).

Finally, this study revealed both patients and healthcare personnel lacking sufficient security routines for passwords. Some use 2FA and biometric authentication when it is offered or selectively, they all admit to using weak passwords and re-using passwords, and some do not always use passwords for their devices. Patients express they would be more conscious about security if insulin injections were controlled by an app. Findings suggest that if diabetes IoT required 2FA or biometric authentication to access it, most patients and healthcare personnel would use it. If it was made mandatory, they would be forced to use it. The healthcare institution where the healthcare personnel in this study work has increased their focus on privacy and security and offers an annual mandatory e-learning course. They do, however, not provide but a best practice guide to how to handle passwords, which has been described as one of the most crucial entry points by previous studies and simulated attacks (Riksrevisjonen 2020). Additionally, healthcare personnel provided a variation of different explanations to their routines on password security and account sharing, suggesting there is no unified guidelines putting much responsibility on the individual healthcare personnel. Healthcare institutions are advised to follow Greene's (2020), and make sure to continually educate their employees about cybersecurity, providing best practice guidelines for security, and making 2FA mandatory, to reduce the risk of attacks and secure patient privacy.

6. Conclusion and opportunities for future research

By investigating the relationship between the potential improved life-quality from using diabetes IoT and the challenges regarding privacy and cyberthreats, several discoveries with important implications for research and practice were made. Results from this study show that diabetic patients experience a drastic increased life-quality from using IoT in diabetes treatment, confirming the implications of earlier studies. Healthcare personnel confirmed HbA1c to stabilize, which contributes to reducing the risk of developing related diseases, and experiencing patients describing they feel like they do not have diabetes anymore. Especially the use of closed loop solutions has been described by both patients and healthcare personnel to improving patients' life-quality. Further, it suggests that neither patients nor healthcare personnel are concerned about patient privacy or threats against diabetes IoT, despite an increased cyberthreats in the healthcare sector. Findings revealed neither three stakeholder groups consider diabetes data to be sensitive data. Both patients and healthcare personnel want to utilize the technological advantages by combining clinical data with real-time IoT data. For this to happen, the industry addresses a pressing matter for the discussion about data ownership generated by such devices and revision of privacy regulations that makes it easier for all Norwegian healthcare regions to interpret, comply, and act upon equally, to utilize the technology available and ensure diabetes patients all over the country have the same opportunities when it comes to patient care.

6.1 Implications

6.1.1 Implications for research

This research provides new insights in IoT adoption issues related to cybersecurity in the healthcare sector, as well as contributes to the discussion of patient privacy. While most of the existing research has examined the advantages of IoT and privacy challenges in the healthcare sector separately, this research has through a multiple-case study design investigated the relationship between them. The findings enrichen the theory with how the impact of IoT in diabetes treatment is evaluated against patient privacy. It also shed lights on research gaps that future research is advised to investigate further to add to the existing body of knowledge about the use of IoT in healthcare.

6.1.2 Implications for practice

This study contributes to practice by offering the perspective of various stakeholders involved with IoT in diabetes treatment and cybersecurity questions related to this. Hence, the findings could be useful for other stakeholders who wish to identify how to enhance cybersecurity in the healthcare sector. Moreover, the findings could assist leaders in healthcare institutions, organizations, and the government to address the debate about data ownership, discuss the differences in how Norwegian healthcare regions interpret privacy regulations and utilize technology, and be more educated about cybersecurity.

6.2 Limitations and future research

The conducted study holds four important limitations that must be addressed:

1) First and foremost, the number of interviews conducted in each stakeholder group might not be extensive enough to generalize the findings. Despite reaching data saturation for in interview three with the first two stakeholder groups, it is possible that the findings would have been more varied findings if the participants had larger variation in characteristics such as age, gender, city of residence and workplace, education, ethnicity, etc. Data saturation was not reached with the industry representative group, which could have affected the results of this study. Additionally, this group could have been divided further into three cases and included more participants in each group. Further, the study is conducted in Norway, where citizens generally have a relaxed attitude towards data privacy and security (Sajid and Haddara 2016), suggesting other results might be found if a similar study was conducted within another context such as country or

culture. Hence, future research should widen the scope to include more variety, larger samples, and different countries, to attempt to shed light on new findings. Moreover, other studies should study the impact of IoT in diabetes treatment in other Norwegian healthcare regions to investigate how potential different utilization of exiting technology affects patient care.

2) The landscape of IoT-technology, cybersecurity, and human behavior, as well as the combinations in between go beyond the scope of this thesis. Themes such as technical specifications and architectures that secures IoT-technology, the variety of potential attacks, legal challenges, and technology adoption theory have not been described in detail. Future research is advised to investigating these factors more in-depth, to provide richer understanding to patients and healthcare personnel's security behavior and technical solutions that could assist in ensuring safety.

3) Other interesting discussions emerged during the interviews but was not included due to being outside the thesis' scope. However, it was found to have potential for future research. The diabetes doctors argued despite the benefits from technological development, they would instead relocate some of the money granted to diabetes treatment to hire more diabetes nurses, as the information they give and time they spend with patients is an essential part of the total package of quality patient care. They further claimed that more patients could benefit more from learning more functionality in their current equipment than re-learning functionality they already know in new equipment that have minor improvements in technical specifications, and that the money saved on new equipment could be used to hire more nurses. Future research is advised to explore both how money in diabetes treatment can be distributed most efficient and investigate the correlation between enhanced clinical data when upgrading IoT equipment versus taking all functionality to use.

4) Lastly, the complex theories and concepts have been interpreted, simplified, and synthesized by the author in an attempt to bring key concepts together and to draw on them to provide new insights to the researched topic. Even though the author has kept in mind the traps of bias and taken precautions to minimize them, there is always a chance of bias occurring when working with qualitative data. Additionally, the interviews were conducted in Norwegian before the transcripts were translated to English. Hence, subtle connections and details in the existing literature and interviews that could have provided greater discussion may have been lost.

References

Abdollahi, Jafar, Babak Nouri Moghaddam, and Mehdi Effat Parvar. 2019. “Improving Diabetes Diagnosis in Smart Health Using Genetic-Based Ensemble Learning Algorithm Approach to IoT Infrastructure” 1 (2): 26–33.

Ahn, David T., and Rachel Stahl. 2019. “Is There an App for That? The Pros and Cons of Diabetes Smartphone Apps and How to Integrate Them Into Clinical Practice.” *Diabetes Spectrum* 32 (3): 231–36. https://doi.org/10.2337/ds18-0101.

Alaba, Fadele Ayotunde, Mazliza Othman, Ibrahim Abaker Targio Hashem, and Faiz Alotaibi. 2017. “Internet of Things Security: A Survey.” *Journal of Network and Computer Applications* 88 (June): 10–28. https://doi.org/10.1016/j.jnca.2017.04.002.

Alhirabi, Nada, Omer Rana, and Charith Perera. 2021. “Security and Privacy Requirements for the Internet of Things: A Survey.” *ACM Transactions on Internet of Things* 2 (1): 1–37. https://doi.org/10.1145/3437537.

Al-Taee, Majid A., Waleed Al-Nuaimy, Ali Al-Ataby, Zahra J. Muhsin, and Suhail N. Abood. 2015. “Mobile Health Platform for Diabetes Management Based on the Internet-of-Things.” In *2015 IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT)*, 1–5. Amman, Jordan: IEEE. https://doi.org/10.1109/AEECT.2015.7360551.

Alvarez, Sarah L., Stephanie L. Baller, and Anthony Walton. 2021. “Who Owns Your Health Data? Two Interventions Addressing Data of Wearable Health Devices among Young Adults and Future Health Clinicians.” *Journal of Consumer Health on the Internet* 25 (1): 35–49. https://doi.org/10.1080/15398285.2020.1852386.

Amaraweera, Suvini P., and Malka N. Halgamuge. 2019. “Internet of Things in the Healthcare Sector: Overview of Security and Privacy Issues.” In *Security, Privacy and Trust in the IoT Environment*, edited by Zaigham Mahmood, 153–79. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-18075-1_8.

Armstrong, David G., David N. Kleidermacher, David C. Klonoff, and Marvin J. Slepian. 2016. “Cybersecurity Regulation of Wireless Devices for Performance and Assurance in the Age of ‘Medjacking.’” *Journal of Diabetes Science and Technology* 10 (2): 435–38. https://doi.org/10.1177/1932296815602100.

Atzori, Luigi, Antonio Iera, and Giacomo Morabito. 2010. “The Internet of Things: A Survey.” *Computer Networks* 54 (15): 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010.

Barati, Masoud, and Omer Rana. 2020. “Enhancing User Privacy in IoT: Integration of GDPR and Blockchain.” In *Blockchain and Trustworthy Systems*, edited by Zibin Zheng, Hong-Ning Dai, Mingdong Tang, and Xiangping Chen, 1156:322–35. Communications in Computer and Information Science. Singapore: Springer Singapore. https://doi.org/10.1007/978-981-15-2777-7_26.

Bhatt, Yesha, and Chintan Bhatt. 2017. “Internet of Things in HealthCare.” *Internet of Things and Big Data Technologies for Next Generation Healthcare*, Studies in Big Data, 23:

13–33. https://doi.org/10.1007/978-3-319-49736-5_2.

Bide, Pramod, and Abhishek Padalkar. 2020. “Survey on Diabetes Mellitus and Incorporation of Big Data, Machine Learning and IoT to Mitigate It.” In *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*, 1–10. Coimbatore, India: IEEE. https://doi.org/10.1109/ICACCS48705.2020.9074202.

Britton, Katherine E., and Jennifer D. Britton-Colonnese. 2017. “Privacy and Security Issues Surrounding the Protection of Data Generated by Continuous Glucose Monitors.” *Journal of Diabetes Science and Technology* 11 (2): 216–19. https://doi.org/10.1177/1932296816681585.

Bruvoll, Janita A., Aasmund Thuv, and Geir Enemo. 2020. “Håndtering Av IKT-Sikkerhetshendelsene i Helse Sør-Øst Og Fylkesmannsembetene - En Vurdering.” 20/01560. Forsvarets forskningsinstitutt.

Bryman, Alan. 2012. *Social Research Methods*. 4th ed. Oxford ; New York: Oxford University Press.

Chander, Anupam. 2020. “Is Data Localization a Solution for Schrems II?” *Journal of International Economic Law* 23 (3): 771–84. https://doi.org/10.1093/jiel/jgaa024.

Chouffani, Reda. 2020. “Future of IoT in Healthcare Brought into Sharp Focus.” *IoT Agenda*, July 2, 2020. https://internetofthingsagenda.techtarget.com/feature/Can-we-expect-the-Internet-of-Things-in-healthcare.

Cleveland, Signe Marie, and Moutaz Haddara. 2021. “IoT for Diabetics: A User Perspective.” In *Intelligent Computing*, edited by Kohei Arai, 285:161–72. Lecture Notes in Networks and Systems. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-80129-8_13.

Conde, Cristina Fernandez. 2021. “A Quick Guide to Case Studies.” https://youthdatingviolence.prevnet.ca/wp-content/uploads/2021/03/Guide-to-Case-Studies-fnl.pdf.

Datatilsynet. 2020. “Utfyllende Veiledning Om Schrems II.” Datatilsynet. November 11, 2020. https://www.datatilsynet.no/regelverk-og-verktoy/internasjonalt/retningslinjer-og-uttalelser-fra-personvernradet/utfyllende-veiledning-om-schrems-ii/.

Dexcom. 2022. “What Is CGM?” 2022. https://www.dexcom.com/continuous-glucose-monitoring.

Diabetesforbundet. 2021b. “Insulinpumper Og Sensorer.” March 11, 2021. https://www.diabetes.no/diabetes-type-1/behandling/insulinpumper-og-sensorer/.

———. 2022a. “Diabetes Type 1.” 2022. https://www.diabetes.no/diabetes-type-1/.

Diasend. 2020. “What Is Diasend?” 2020. https://support.diasend.com/hc/en-us/articles/211990605-What-is-diasend.

DNV. 2022. “ISO/IEC 27001 - Ledelsessystem for Informasjonssikkerhet.” 2022. https://www.dnv.no/services/iso-iec-27001-ledelsessystem-for-informasjonssikkerhet-33652.

Dubé, Line, and Guy Paré. 2003. “Rigor in Information Systems Positivist Case Research: Current Practices, Trends, and Recommendations.” *MIS Quarterly* 27 (4): 597. https://doi.org/10.2307/30036550.

Eisenhardt, Kathleen M. 1989. “Building Theories from Case Study Research.” *Academy of Management Review* 14 (4): 532–50. https://doi.org/10.5465/amr.1989.4308385.

Fearn, Nicholas. 2021. “How Can Healthcare Organisations Fight Increased Cyber Crime in 2021?” *ComputerWeekly*, January 21, 2021. https://www.computerweekly.com/feature/How-can-healthcare-organisations-fight-increased-cyber-crime-in-2021.

FHI. 2020. “Nye Tall Om Hvor Mange Som Har Diabetes i Norge.” Folkehelseinstituttet. November 13, 2020. https://www.fhi.no/nyheter/2020/nye-tall-om-hvor-mange-som-har-diabetes-i-norge/.

Gómez, Jorge, Byron Oviedo, and Emilio Zhuma. 2016. “Patient Monitoring System Based on Internet of Things.” *Procedia Computer Science* 83: 90–97. https://doi.org/10.1016/j.procs.2016.04.103.

Greene, Michael. 2020. “Why Healthcare Providers Must Take Action to Eliminate Cybersecurity Risks.” *IoT Agenda*, September 18, 2020. https://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/Why-healthcare-providers-must-take-action-to-eliminate-cybersecurity-risks.

Gripsrud, Geir, Ulf Henning Olsson, and Ragnhild Silkoset. 2016. *Metode og dataanalyse beslutningsstøtte for bedrifter ved bruk av JMP, Excel og SPSS*. Oslo: Cappelen Damm akademisk.

Gubbi, Jayavardhana, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. 2013. “Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions.” *Future Generation Computer Systems* 29 (7): 1645–60. https://doi.org/10.1016/j.future.2013.01.010.

Harvard Medical School. 2022. “Type 1 Diabetes Mellitus.” January 13, 2022. https://www.health.harvard.edu/a_to_z/type-1-diabetes-mellitus-a-to-z.

Hernæs, Tina. 2022. “100 År Siden Leonard Thompson Sto Opp Fra de Døde.” *Sykepleien*, February 11, 2022.

Islam, S. M. Riazul, Daehan Kwak, Md. Humaun Kabir, Mahmud Hossain, and Kyung-Sup Kwak. 2015. “The Internet of Things for Health Care: A Comprehensive Survey.” *IEEE Access* 3: 678–708. https://doi.org/10.1109/ACCESS.2015.2437951.

Istepanian, R. S. H., S. Hu, N. Y. Philip, and A. Sungoor. 2011. “The Potential of Internet of M-Health Things ‘m-IoT’ for Non-Invasive Glucose Level Sensing.” In *2011 Annual*

International Conference of the IEEE Engineering in Medicine and Biology Society, 5264–66. Boston, MA: IEEE. https://doi.org/10.1109/IEMBS.2011.6091302.

Kaplan, Bonnie, and Dennis Duchon. 1988. “Combining Qualitative and Quantitative Methods in Information Systems Research: A Case Study.” *MIS Quarterly* 12 (4): 571. https://doi.org/10.2307/249133.

Kintzlinger, Matan, and Nir Nissim. 2019. “Keep an Eye on Your Personal Belongings! The Security of Personal Medical Devices and Their Ecosystems.” *Journal of Biomedical Informatics* 95 (July): 103233. https://doi.org/10.1016/j.jbi.2019.103233.

Kjærnli, Arild. 2021. “Beskyttelse Mot Cyberangrep Er Kritisk.” *Nek.No*, February 19, 2021. https://www.nek.no/beskyttelse-mot-cyberangrep-er-kritisk/.

Klonoff, David C., David Kerr, and Dave Kleidermacher. 2017. “Now Is the Time for a Security and Safety Standard for Consumer Smartphones Controlling Diabetes Devices.” *Journal of Diabetes Science and Technology* 11 (5): 870–73. https://doi.org/10.1177/1932296817723259.

Klonoff, David C., Trisha Shang, and Jennifer Zhang. 2021. “Automated Insulin Dosing Systems or Automated Insulin Delivery Systems? It Is Time for Consistency.” *Journal of Diabetes Science and Technology* 15 (2): 211–13. https://doi.org/10.1177/1932296821993498.

Kristiania University College. 2022. “Forskningsetikk Og Personvern.” 2022. https://www.kristiania.no/forskning/forskningsstotte/forskningsetikk--og-personvern/.

Lerman, Leon. 2020. “Where Healthcare IoT Is Headed in 2020.” *IoT Agenda*, March 9, 2020. https://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/Where-healthcare-IoT-is-headed-in-2020?_ga=2.102904072.909278353.1590313670-1630110317.1590313670.

Loideain, Nóra Ni. 2019. “A Port in the Data-Sharing Storm: The GDPR and the Internet of Things.” *Journal of Cyber Policy* 4 (2): 178–96. https://doi.org/10.1080/23738871.2019.1635176.

Longva, Anne Marit, and Moutaz Haddara. 2019. “How Can IoT Improve the Life-Quality of Diabetes Patients?” Edited by N. Mastorakis, V. Mladenov, and A. Bulucea. *MATEC Web of Conferences* 292: 03016. https://doi.org/10.1051/matecconf/201929203016.

Myers, Michael D. 1997. “Qualitative Research in Information Systems.” *MIS Quarterly* 21 (2): 241. https://doi.org/10.2307/249422.

———. 1999. “Investigating Information Systems with Ethnographic Research.” *Communications of the Association for Information Systems* 2. https://doi.org/10.17705/1CAIS.00223.

Nasjonal Sikkerhetsmyndighet. 2022. “Risiko 2022.” https://nsm.no/getfile.php/137798-1644424185/Filer/Dokumenter/Rapporter/NSM_rapport_final_online_enekeltsider.pdf.

NHI. 2020. “Høyt Blodsukker Ved Diabetes Type 1.” Norsk Helseinformatikk. December 8, 2020. https://nhi.no/sykdommer/hormoner-og-naring/diabetes-type-1/hoyt-blodsukker-hyperglykemi-ved-type-1-diabetes/.

———. 2021. “Lavt Blodsukker, Hypoglykemi, Ved Diabetes Mellitus.” Norsk Helseinformatikk. July 15, 2021. https://nhi.no/sykdommer/hormoner-og-naring/diabetes-type-1/lavt-blodsukker-hypoglykemi-ved-diabetes/.

Norsk helsenett. 2021. “Situasjonsbilde 2021.” https://www.nhn.no/Personvern-og-informasjonssikkerhet/helsecert/situasjonsbilde-2021.

NSD. 2022. “Oppslagsverk for Personvern i Forskning.” Norsk Senter for Forskningsdata. 2022. https://www.nsd.no/personverntjenester/oppslagsverk-for-personvern-i-forskning/.

Oates, Briony J. 2006. *Researching Information Systems and Computing*. London; Thousand Oaks, Calif: SAGE Publications.

Patil, Harsh Kupwade, and Ravi Seshadri. 2014. “Big Data Security and Privacy Issues in Healthcare.” In *2014 IEEE International Congress on Big Data*, 762–65. Anchorage, AK: IEEE. https://doi.org/10.1109/BigData.Congress.2014.112.

Patton, Michael Quinn. 2015. *Qualitative Research & Evaluation Methods: Integrating Theory and Practice*. Fourth edition. Thousand Oaks, California: SAGE Publications, Inc.

Perera, Charith, Arkady Zaslavsky, Peter Christen, and Dimitrios Georgakopoulos. 2014. “Context Aware Computing for The Internet of Things: A Survey.” *IEEE Communications Surveys & Tutorials* 16 (1): 414–54. https://doi.org/10.1109/SURV.2013.042313.00197.

Putch, Kristen. 2021. “Healthcare Security Services Firms Tackle Ransomware Spike.” *TechTarget*, February 26, 2021. https://searchitchannel.techtarget.com/feature/Healthcare-security-services-firms-tackle-ransomware-spike.

Rehman, Arshia, Saeeda Naz, and Imran Razzak. 2021. “Leveraging Big Data Analytics in Healthcare Enhancement: Trends, Challenges and Opportunities.” *Multimedia Systems*, January. https://doi.org/10.1007/s00530-020-00736-8.

REK. 2022. “Om å Søke REK.” Rekportalen. 2022. https://rekportalen.no/#hjem/søke_REK.

Riksrevisjonen. 2020. “Riksrevisjonens Undersøkelse Av Helseforetakenes Forebygging Av Angrep Mot Sine IKT-Systemer.” ISBN-978-82-8229-489-8.

Rodbard, David. 2016. “Continuous Glucose Monitoring: A Review of Successes, Challenges, and Opportunities.” *Diabetes Technology & Therapeutics* 18 (S2): S2-3-S2-13. https://doi.org/10.1089/dia.2015.0417.

Sajid, Ozaire, and Moutaz Haddara. 2016. “NFC Mobile Payments: Are We Ready for Them?” In *2016 SAI Computing Conference (SAI)*, 960–67. London, United Kingdom: IEEE. https://doi.org/10.1109/SAI.2016.7556096.

Saltzstein, William. 2020. “Bluetooth Wireless Technology Cybersecurity and Diabetes Technology Devices.” *Journal of Diabetes Science and Technology* 14 (6): 1111–15. https://doi.org/10.1177/1932296819864416.

Seglsten, Per Helge. 2021. “Check Point-Rapport: 458 Cyberangrep Mot Norske Organisasjoner Hver Uke.” *Digi.No*, October 11, 2021. https://www.digi.no/artikler/check-point-rapport-458-cyberangrep-mot-norske-organisasjoner-hver-uke/514041?key=SMAzPbE6.

Shahid, Jahanzeb, Rizwan Ahmad, Adnan K. Kiani, Tahir Ahmad, Saqib Saeed, and Abdullah M. Almuhaideb. 2022. “Data Protection and Privacy of the Internet of Healthcare Things (IoHTs).” *Applied Sciences* 12 (4): 1927. https://doi.org/10.3390/app12041927.

Tandem. 2022. “Software & Apps.” Tandem Diabetes Care. 2022. https://www.tandemdiabetes.com/products/software-apps.

Thomas, Gary. 2021. *How to Do Your Case Study*. Third edition. London ; Los Angeles: SAGE.

Walsham, G. 1995. “Interpretive Case Studies in IS Research: Nature and Method.” *European Journal of Information Systems* 4 (2): 74–81. https://doi.org/10.1057/ejis.1995.9.

WHO. 2021. “Diabetes.” World Healthcare Organization. November 10, 2021. https://www.who.int/news-room/fact-sheets/detail/diabetes.

Yin, Robert K. 2016. *Qualitative Research from Start to Finish*. Second edition. Research Methods. New York London: The Guilford Press.

———. 2018. *Case Study Research and Applications: Design and Methods*. Sixth edition. Los Angeles: SAGE.

Appendix

Appendix A: Information letter and consent form for patients and healthcare personnel

Vil du delta i forskningsprosjektet: *"The Rise and Falls of IoT for Diabetics: Improved Life Quality vs. Patient Safety"*

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å se på hvordan den antatte økte livskvaliteten ved bruk av IoT diabetesteknologi (slik som insulinpumpe og blodsukkersensor) veies opp mot datasikkerheten knyttet til bruken av denne teknologien i behandling av diabetes type 1. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål

Antallet mennesker som lever med og dør av kritiske, kroniske sykdommer øker for hver år og er et verdensomspennende problem. Heldigvis utvikles det stadig nye teknologier og løsninger som hjelper pasienter å holde sykdommene i sjakk og leve tilnærmet normale liv. Internet of Things (IoT) er en teknologi som knytter fysiske ting til internett og bidrar til effektiv og strømlinjeformet informasjonsoverføring. IoT brukes i mange løsninger for å monitorere diabetes, slik som trådløse blodsukkersensorer og automatiske insulinpumper. Disse apparatene kan ha stor innvirkning på livskvaliteten til en person med diabetes, men som med all teknologi er det ikke uten risiko. Antallet cyberangrep øker med enorm hastighet, med helsesektoren som det mest attraktive målet, og det tas stadig nye metoder i bruk for å få tak i informasjon og få kontroll over systemer. Personlige medisinske apparater er sårbare for cyberangrep, og setter derfor pasienters personvern og sikkerhet er i fare.

Formålet med dette masterprosjektet er å undersøke hvorvidt IoT-teknologi bidrar til økt livskvalitet for personer med diabetes type 1, tanker rundt cybersikkerhet i behandling av diabetes, og hvordan potensiell økt livskvalitet vektes mot potensielle cyberangrep, fra pasient- og helsepersonellperspektiv.

Hvem er ansvarlig for forskningsprosjektet?

Høyskolen Kristiania er ansvarlig for prosjektet.

Hvorfor får du spørsmål om å delta?

Du er aktuell for å delta i intervju fordi du enten har diabetes type 1 og benytter IoT-teknologi som trådløs blodsukkersensor eller automatisk insulinpumpe, eller fordi du er helsepersonell som jobber med pasienter som har diabetes type 1 og bruker ovennevnte teknologi.

Hva innebærer det for deg å delta?

Hvis du velger å delta i prosjektet innebærer det et intervju som vil ta ca. 1 time. Under intervjuet vil du få spørsmål om dine tanker og erfaringer rundt monitorering og behandling av diabetes type 1, teknologien som benyttes i behandling, og sikkerhet knyttet til bruk av denne teknologien. Det vil altså ikke dreie seg om medisinske spørsmål. Intervjuet vil gjennomføres digitalt, lyden vil tas opp for at opplysningene skal kunne gjengis korrekt i transkribering. Du og eventuell arbeidsplass vil anonymiseres.

Det er frivillig å delta

Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger

Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

Signe Marie Cleveland (masterstudent) samler inn, bearbeider og lagrer data. Moutaz Haddara (veileder) vil ha tilgang på data. Kontaktinformasjon og lydopptak lagres i One Drive tilhørende Høyskolen Kristiania. I transkribert intervju, endelig oppgave og eventuell publikasjon vil du være anonymisert.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?

Opplysningene anonymiseres når prosjektet avsluttes/oppgaven er godkjent, noe som etter planen er juni 2022. Kontaktinformasjon og lydopptak slettes ved endt prosjekt.

Dine rettigheter
Så lenge du kan identifiseres i datamaterialet, har du rett til:

- innsyn i hvilke personopplysninger som er registrert om deg, og å få utlevert en kopi av opplysningene,
- å få rettet personopplysninger om deg,
- å få slettet personopplysninger om deg, og
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger.

Hva gir oss rett til å behandle personopplysninger om deg?
Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra Høyskolen Kristiania har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Hvor kan jeg finne ut mer?
Hvis du har spørsmål til studien, eller ønsker å benytte deg av dine rettigheter, ta kontakt med:

- Høyskolen Kristiania ved Signe Marie Cleveland, clesig16@student.kristiania.no, eller Moutaz Haddara, moutaz.haddara@kristiania.no.
- Vårt personvernombud: personvernombud@kristiania.no

Hvis du har spørsmål knyttet til NSD sin vurdering av prosjektet, kan du ta kontakt med:

- NSD – Norsk senter for forskningsdata AS på epost (personverntjenester@nsd.no) eller på telefon: 55 58 21 17.

Med vennlig hilsen

Moutaz Haddara Signe Marie Cleveland

Moutaz Haddara Signe Marie Cleveland
(Forsker/veileder) (Masterstudent)

Samtykkeerklæring
Jeg har mottatt og forstått informasjon om prosjektet *"The Rise and Falls of IoT for Diabetics: Improved Life Quality vs. Patient Safety"*, og har fått anledning til å stille spørsmål. Jeg samtykker til:

- å delta i intervju

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

----
(Signert av prosjektdeltaker, dato)

Appendix B: Request and information e-mail for industry

Hei,

Mitt navn er Signe Marie Cleveland, og jeg skriver for øyeblikket masteroppgave om diabetesteknologi og forholdet mellom økt livskvalitet og potensielle sikkerhetstrusler, ved Høyskolen Kristiania i Oslo. I den sammenheng lurer jeg på om noen hos dere har tid og anledning til et raskt telefonintervju for å besvare noen spørsmål jeg har vedrørende hvordan dere vurderer sikkerheten til insulinpumper og CGM/sikkerhet og risikobildet innen e-helse/ sikkerhetsvurderinger ved inngåelse av disse avtalene/datasikkerhet for diabetespasienter risikobildet innen e-helse/informasjonssikkerhet og datadeling ved bruk av diabetesteknologi/personvern ved bruk av diabetesteknologi?

Intervjuet vil gjennomføres over telefon, og jeg estimerer at det tar maks. 15 minutter. Jeg er svært fleksibel på tidspunkt, men ønsker gjerne å gjennomføre intervjuet før påske. Jeg forstår at det kan være visse restriksjoner på hvor mye informasjon som kan utleveres, men jeg håper det allikevel vil være mulig å kunne snakke noe generelt om sikkerhetsvurderinger/sikkerhet/utfordringer/personvern. Din identitet og bedrift/arbeidsplass vil holdes anonym.

Jeg kan også legge til at diabetes og teknologien som brukes i behandling er et stort interesseområde for meg. Jeg har allerede publisert en forskningsartikkel om temaet, og masteroppgaven vil på mange måter bli en del 2 eller oppfølging til denne publikasjonen (IoT for Diabetics: A User Perspective, 2021, https://link.springer.com/chapter/10.1007/978-3-030-80129-8_13), med noe mer fokus på sikkerheten og med flere perspektiver, men det forutsetter at jeg får tak i nok personer som vil snakke med meg.

Håper på positiv tilbakemelding!

Med vennlig hilsen,
Signe Marie Cleveland
clesig16@student.kristiania.no
92406620

Appendix C: Interview guide – Patients

First, thank you for taking the time to answer some questions regarding diabetes and your equipment. We will not talk about your measures and dosage, but more about diabetes and the equipment itself, and how you experience living with diabetes and the journey from the diagnosis until today.

The answers will be used as a supplement to literature gathered around the topic, for my Master Thesis in Information Systems at Kristiania University College. You and your answers will be anonymized. Is it okay that I record this interview? The recording will only be used by me for the purpose of transcribing the interview, and only until the end of June 2022 when I have presented my thesis.

The interview is divided into 3 subtopics. First I need some information about you and your diabetes. For the second part I'm going to ask you questions regarding both your previous and current equipment, and we will talk a bit about the journey from being diagnosed until today. The third part is focusing on how you experience the privacy and security of the equipment.

All answers will as mentioned be anonymized, and I am looking for your subjective opinion and thoughts around these topics. I do have some specific questions I would like for you to answer, but I would like us to talk about the topics as a normal conversation, and I will follow up with questions where needed. If there is anything you don't want to answer for any reason just let me know and we will continue to the next question.

Part 1: Personal information
Q1: Tell me about yourself (for getting the conversation going)
Topics that should be covered:

- Age
- Gender
- Occupation

Q2: How old were you when you were diagnosed with Diabetes, and how did you experience this?
Possible follow up with: How do you think your parents experienced it? <- if diagnosed as a child.

Q3: What are your main challenges living with diabetes? Like linked medical conditions, psychological issues, using equipment, etc.

Part 2: Equipment
Q4: What type of equipment did you start out using?
Should include glucose monitoring and how insulin is injected (pump/pen/etc).
Follow up: How did the equipment work, and how did that work for you? How often did you have to measure your glucose levels and inject insulin you reckon?

Q5: What type of equipment do you use today?
Should include CGM and insulin pump.
Follow up: How does the equipment work, and how is this working for you?

Q6: Have you used wireless devices before the ones you are using today?
Follow up: Which, and how would you compare them? Improvement?

Q7: How did you experience the transition from manual to wireless/automated equipment?
Follow up: Were there any concerns? Was it difficult to use? Or start using it? Did you trust the equipment?

Q8: How has your current equipment impacted your life?
Follow up: How do you experience using it? What do you consider the most and least advantageable with it? How could it be enhanced for making living with diabetes easier?

Q9: Do you visit your doctor/hospital more or less after changing to your current equipment?
Follow up: How have the visits changed? Longer/shorter? More/less changes in your "medical strategy"? How do you think it will evolve from here?
Q10: Do you have any concerns regarding your current equipment?
Follow up: Why/why not? If yes, what? If no, what makes it free of concerns? Do you rely on your equipment? Both for it not to break down, and to give accurate and correct measures?

Q11: If you could wish for any adjustments to your current equipment that would improve your life quality, what

would it be?
Should include a reflection on technology innovation, how the equipment could be smarter or more seamless.

Part 3: Privacy and security (some might be covered in questions above)
Q12: Through your equipment, what data about you is registered and stored, and who has access to it?
Follow up: How much personal data, and is it linked directly to your medical record with all other information?

Q13: Do you trust the manufacturer of the equipment?
Follow up: Do you trust that the equipment won't break down, do you trust that your data is not misused?
Q14: Do you have any concerns regarding how the data is stored and who has access to it?
Follow up: How do you think you will be affected if the data gets stolen? Do you think your medical record can be held against you in some cases?

Q15: What happens if your devices are stolen or someone hacks them?
Follow up: What if someone intentionally wants to harm you and steals your device/phone and adjusts your insulin dosage? Worst case.

Q16: What are your thoughts about wearing such devices that are connected to the internet?
Follow up: What if I tell you there are about 450 cyberattacks in Norway each week, the healthcare sector is the most prominent target for cyberattacks, there are reported several successful attacks against wearable medical IoT such as insulin pumps, and Riksrevisjonen were able to get control over the IT systems of the four Regional Health Authorities in Norway through simulated attacks last year, how do you feel about wearing it?

Appendix D: Interview guide – Healthcare personnel

First, thank you for taking the time to answer some questions regarding diabetes equipment and its effect on your patients and your workflow. We will not talk about specific individuals or the medical terms of diabetes today, but your experience of diabetes technology and its evolution. I am mainly interested in the perspective of diabetes type 1.

The answers will be used as a supplement to literature gathered around the topic, for my Master Thesis in Information Systems at Kristiania University College. You and your answers will be anonymized. Is it okay that I record this interview? The recording will only be used by me for the purpose of transcribing the interview, and only until the end of June 2022 when I have presented my thesis.

The interview is divided into 3 subtopics. First I need some information about you and your career within diabetes care. For the second part I'm going to ask you questions regarding diabetes technology and how it affects your patients and your workflow. The third part is focusing on how you experience the privacy and security of the equipment.

All answers will as mentioned be anonymized, and I am looking for your subjective opinion and thoughts around these topics. I do have some specific questions I would like for you to answer, but I would like us to talk about the topics as a normal conversation, and I will follow up with questions where needed. If there is anything you don't want to answer for any reason just let me know and we will continue to the next question.

Part 1: Professional information
Q1: Tell me about your professional self (for getting the conversation going)
Topics that should be covered:

- Brief timeline as a healthcare professional
- Current occupation
- Time spent working with diabetes patients

Q2: What got you interested in working with diabetes patients?

Q3: What do you see as the most challenging for patients with diabetes? Like linked medical conditions, psychological issues, using equipment, etc.

Part 2: Diabetes technology
Q4: How long have you been working with this kind of technological diabetes devices, such as CGM and insulin pumps?
Follow up: Are you working with different brands or mainly just one type of each?
Q5: What are your thoughts about CGM and insulin pumps?
Should include if the person is positive or negative to the technology, then follow up with why this attitude.

Q6: Which patients do you reccomend start using CGM and insulin pumps?
Should include if patients are newly diagnosed, their age, possible limitations.
Follow up: Why shouldn't all diabetics use it? Are there some cases where you only recommend one of the two, why?

Q7: How do you experience a patient's transition from manual to automatic devices?
Follow up: What are the most prominent concerns or difficulties? How does it impact their diabetes itself, but also life quality and related diseases?

Q8: How has this transition impacted your work situation?
Should include a reflection on workload, efficiency, patient relationships and visits.
Follow up: How do you think the patient visits will evolve with the technology?

Q9: What do you see as the most challenging part with this type of equipment?
Should include possible technical challenges for patients or professionals, user difficulties, limitations with equipment, etc.
Follow up: How many patients experience malfunctioning equipment?
Q10: If you could wish for any adjustments to the current equipment that would improve your patients' life quality, what would it be?
Should include a reflection on technology innovation, how the equipment could be smarter or more seamless.

Part 3: Privacy and security
Q11: How does GDPR fit into the use of these devices?
Follow up: Has GDPR made it more difficult to recommend IoT technology for the patients, are you strictly following GDPR in terms of consent and data sharing?

Q12: Through the equipment, what type of data about the patient is registered and stored, and who has access to it?
Follow up: How much personal data, and is it linked directly to the patients' medical record with all other information? Do you use/need all the data that is stored in order to provide quality care for the patient?

Q13: Do you trust the manufacturer of the equipment?
Follow up: Do you trust that the equipment won't break down, do you trust that the patients' data is not misused?

Q14: Who is responsible for ensuring the patient's data is protected?
Follow up: Healthcare facility/manufacturer?

Q15: What kind of safety procedures do you have in your workplace when it comes to patient data?
Follow up: What does it take to look up a patient's information?

Q16: Do you have any concerns regarding how the data is stored and who has access to it, in terms of your patients' safety and privacy?
Follow up: How do you think the patients will be affected if the data gets stolen? Do you think their medical record can be held against them in some cases?

Q17: Have you experienced a cyberattack at your workplace? If yes, how did this affect the patients? What were your concerns?

Q18: What do you think happens if the devices are stolen or someone hacks them?
Follow up: What if someone intentionally wants to harm the patient and steals their device/phone and adjusts the insulin dosage? Worst case.

Q19: What are your thoughts about patients wearing such devices that are connected to the Internet and constantly generating data?
Follow up: What if I tell you there are about 450 cyberattacks in Norway each week, the healthcare sector is the most prominent target for cyberattacks, there are reported several successful attacks against wearable medical IoT such as insulin pumps, and Riksrevisjonen were able to get control over the IT systems of the four Regional Health Authorities in Norway through simulated attacks last year, does it make you concerned about your patients?

Appendix E: Interview guide – Industry representatives

Note: This is a summary of all questions asked the different industry representatives. As they have different specializations, they have received different combinations of these questions in addition to questions that were posed as a natural response during the conversation.

First, thank you for taking the time to answer some questions regarding diabetes equipment and security related questions. The answers will be used as a supplement to literature gathered around the topic and interviews with diabetes patients and healthcare personnel, for my Master Thesis in Information Systems at Kristiania University College. You and your answers will be anonymized.

I do have some specific questions I would like for you to answer, but I would like us to talk about the topics as a normal conversation, and I will follow up with questions where needed. I really appreciate getting your perspective and whatever information you can give me on this topic, and I understand some of the information I'm seeking might be confidential, so please just let me know if there are questions you cannot answer, and we'll move on to the next one.

Q1: First, can you describe your role or area of expertise within the company?

Q2: How do you perceive the landscape of cyber threats in the healthcare sector?
Follow up: What are the main threats? Is there reason to be worried?

Q3: How do you percieve Norwegian patients, healthcare personnel and healthcare institutions' precautions regarding cyber security?
Follow up: How could it be improved, and by whom? Do you think they are critical enough?

Q4: How do you perceive Norwegian privacy/security/safety regulations for data management/data sharing/approving equipment?
Follow up: Patients and healthcare personnel perceive it as to strict, is it?

Q5: How do you perceive the risk of medical equipment being attacked by cyber criminals?
Follow up: What do you think would be the target and goal for those attacks?

Q6: How is this type of equipment and connected data management system secured?

Q7: How often do you experience errors of malfunctions?
Follow up: Who is responsible it this happens? What are the consequences?

Q8: Who owns the data generated by these systems?

Q9: Is there a difference between diabetes technology and other medical technology when it comes to privacy and security?