Erik Stol Øyan

Cybersecurity considerations in the procurement process of digital medical equipment at Norwegian hospitals

Master's thesis in Experience-based Master in Information Security
Supervisor: Maria Bartnes
May 2022

Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

Erik Stol Øyan

Cybersecurity considerations in the procurement process of digital medical equipment at Norwegian hospitals

Master's thesis in Experience-based Master in Information Security
Supervisor: Maria Bartnes
May 2022

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

Title: Cybersecurity considerations in the procurement process of digital medical equipment at Norwegian hospitals

Student: Erik Stol Øyan

Problem description:

Over the last years, several hospitals have been hit by cyberattacks, resulting in unwanted disruption of daily operations. This poses a threat to patient treatment, which in the worst case can lead to loss of life. Additionally, it poses a threat towards patient privacy. Along with the general digitization of our society, hospitals are increasingly using more digital medical equipment in patient treatment, which expands the potential attack surface of cybercriminals. Hence, securing this equipment is an important part of the cybersecurity work that should be conducted at Norwegian hospitals. Implementing security controls that enable you take the right precautions can contribute to elevating the security posture of an organization, which in turn can aid in reducing the potential attack-surface.

Following a qualitative research approach, this thesis seeks to investigate and understand how aligned Norwegian hospitals are with well-known cybersecurity frameworks when it comes to cybersecurity considerations in the procurement process of digital medical equipment. Additionally, the thesis will comment on any potential improvements that are observed in the procurement process at Norwegian hospitals today, if any. Interviews will be conducted to gather information from different hospitals, so that something can be said in general regarding the cybersecurity considerations that are taken in the procurement process of digital medical equipment at Norwegian hospitals.

The problem statement for this Master thesis is to investigate how aligned Norwegian hospitals are with well-known cybersecurity frameworks when it comes to cybersecurity considerations in the procurement process of digital medical equipment.

Supervisor: Maria Bartnes, NTNU / SINTEF

Abstract

The health care services are considered a part of the critical societal infrastructure in Norway, which should be protected to safeguard secure patient treatment. Norwegian health care services are increasing their use of technology in patient treatment, and information that digital medical equipment provides often plays an important part contributing to decision-making processes among health care personnel. At the same time, cybercrime is rapidly increasing; the Norwegian National Security Authority (NSM) reports that threat actors increasingly exploit vulnerabilities, without considering the potential consequences of their actions. Norwegian hospitals have to a certain extent been shielded from this type of activity, but the increased interest from cybercriminals in easy-to-sell health records have made them an attractive target. To secure and protect health records is therefore an important part of the cybersecurity work that should be performed at hospitals.

Among the areas where cybersecurity should be considered, is the procurement process of digital medical equipment. Looking at the lifecycle of equipment, the procurement process can contribute to create a foundation for securing equipment later in the device lifecycle, by selecting vendors that deliver equipment with adequate built-in security measures. In other words, choosing the right equipment contributes to safeguarding the infrastructure, and consequently, the safety and privacy of the patients. To investigate the state of art at Norwegian hospitals, the following problem statement has been prepared to elucidate the topic: *Which cybersecurity considerations are taken in the procurement process of digital medical equipment at Norwegian hospitals?* The problem statement is supported by three research questions that will investigate which cybersecurity considerations that should be taken in the procurement process according to well-known frameworks and best-practices, which cybersecurity considerations that are taken in the procurement process of digital medical equipment at Norwegian hospitals today, and finally, what can be done to improve the current procurement practice of digital medical equipment.

The thesis includes a theoretical part where findings from Norwegian Official Report and reports by the Office of the Auditor General are highlighted, and recommended cybersecurity considerations in the procurement process according to well-known frameworks are listed.

This Master thesis is based on a qualitative research method where data have been collected through a literature study and six semi-structured interviews with representatives from three different health regions and one independent hospital.

The result of the thesis reveals a significant difference in maturity across the health regions, where some participants inform that they have defined processes with dedicated roles and responsibilities that plan procurements, while other health regions experience that they often are involved only after equipment is procured, which in turn forces them to implement compensating security measures in cases where procured equipment has inadequate cybersecurity measures.

The Master thesis concludes that although all the participants in the study informs that they have prepared a set of cybersecurity considerations and requirements, some experience that these considerations are not taken into account due to cybersecurity competence being excluded from the procurement process. This problem seems to stem from the fact that Norwegian health regions and hospitals are somewhat left alone to

figure out how to build a solid procurement process that considers all stakeholders, instead of being provided with a suggested framework for procuring equipment that safeguards cybersecurity through dedicated roles and responsibilities. Therefore, a suggested model for procuring digital medical equipment has been created.

Preface

This Master thesis is marking the end of the Experience-based Master in Information Security at the Norwegian Institute for Technology and Science (NTNU). The work writing this thesis started in summer 2021 and has been both a challenging and educational process until completion in spring 2022. Through working with this Master thesis, I have gained increased insight, knowledge, and understanding of a series of different topics, in addition to the research process and the important role it plays when conducting research. The Master thesis gives a total of 30 study points in IMT4905 – Experience-based Master's Thesis.

The initial idea for this Master thesis came during the IMT4215 Specialization Project course during spring 2021, where I wrote about lifecycle management of IoT devices. During this course, I discovered that although there are four overarching phases of lifecycle management, the procurement phase is the most important, as it sets the precedence for which cybersecurity properties the procured hardware has, consequently creating the foundation for the operational, management and disposal phase. During the summer of 2021, my supervisor and I discussed who might benefit from a project on cybersecurity in the procurement process, and we agreed to focus on the health sector due to its important role and contribution in Norwegian society.

I would like to thank my supervisor Maria Bartnes for valuable support and feedback throughout the master thesis, and my family for the continuous support.

Table of contents

List of figures

List of tables

1 Introduction

In 1964, BBC aired a television show called *The Knowledge Explosion*, where they visualized the city of the future. In episode six of the first series, the following question was raised:

> *"What remains for science to do? How will it affect our lives?"*

What followed, was a series of predictions made by Arthur C. Clarke, among them the prediction of internet and communications technology. Additionally, he said that "*one day, we may have brain surgeons in Edinburgh operating on patients in New Zealand*", which might be made possible by 5G technology today, and that "*in the future, we can be in instant contact with each other, wherever we may be, where we can contact our friends anywhere on earth even though we don't know their actual physical location*" (BBC, 1964).

Since then, the digitalization of our society has grown immensely, and technology has now become a natural, integral part of our society. The benefits of technology are huge – the rapid innovation and adoption entails a continuously increase in productivity and efficiency. This is also true for the health sector, where patient journal systems and digital medical equipment such as CT scan can be used to quickly diagnose patients and provide them with the right treatment. Although technology might not the only contributor, there is reason to believe it plays an important role in for instance decreasing the average number of days that patients stay in hospital, which in Norway has been reduced from 7,5 days in 1989 to 4,2 days in 2016 (Statistisk Sentralbyrå, 2016).

As society continues to adopt and utilize technology, organizations and businesses become more reliant on this technology. Information used in decision-making processes are gathered, stored, and processed in information technology systems. However, this information is not only valuable to the organizations and businesses that owns the information, but also for cyber criminals. Throughout history, crime has evolved with society, and so is the case for cyber-crime. Although the procedures might be vastly different from only 30 years ago, many of the techniques are still the same. The trojan horse is perhaps the best example, referring to when the Greeks built a wooden horse to get inside the city walls of Troy to take the city. The Trojans believed the horse to be a gift from the Gods, and brought it inside the walls, where soldiers hiding inside the horse let the other Greek soldiers in. This technique is widely recognized within the cyber domain as well, by disguising something malicious as a valuable asset, such as a file or software.

The cyber threat landscape is rapidly changing along with the evolution of technology and, unfortunately, it is not only cyber criminals that pose a threat to society and socially critical services. On the 23rd of December 2015, the electricity suddenly disappeared for over 230000 consumers in Ukraine and remained unavailable for up to six hours (Finkle, 2016). The U.S. cyber intelligence firm iSight attributed the attack to a hacker organization called Sandworm, which has ties to the Russian government. There have also been incidents in Norway, like the hack against the Southern and Eastern Regional Health Authority in 2018, where patient information was leaked (NorSIS, 2018), and against the Storting in Norway, where data was exfiltrated (Utenriksdepartementet, 2021). The attack against the Storting was later attributed to a Chinese hacker organization, and the Chinese ambassador had to answer to the Norwegian foreign minister (Furuly, 2021).

There are many other examples as well, which emphasizes the importance of one of cybersecurity's repeated mantras: safeguarding the confidentiality, integrity, and availability of information. Therefore, this thesis will investigate how hospitals can better protect themselves by taking the necessary cybersecurity precautions in the procurement process of digital medical equipment, and consequently increase their resilience towards cyberattacks by reducing their attack surface. Clinical needs drive innovation and purchases of digital medical equipment, however, limited cybersecurity awareness or even the absence of a defined procurement process could lead to purchases of insecure digital medical equipment which consequently could leave hospitals vulnerable to cyberattacks (Schwartz et al., 2018). Therefore, devices such as digital medical equipment need to be managed, and an effective device management plan starts at the procurement stage (Coronado and Wong, 2014). Unfortunately, cybersecurity is rarely at the top of the list (sometimes not even on the list) of considerations when procuring digital medical equipment, and there are numerous stakeholders that have clear expectations regarding the functionality, rather than the security (Rabinowitz, 2018).

1.1 Purpose

The purpose of this master thesis is to enhance the Norwegian hospitals' cybersecurity maturity and resilience towards cybercriminals, through improving the cybersecurity in the procurement process of digital medical equipment. This master thesis presents concrete improvement proposals for the procurement process of digital medical equipment. The foundation for these proposals comes from investigating which cybersecurity considerations that are taken in the procurement process of digital medical equipment at Norwegian hospitals today, and how aligned these considerations are with well-known frameworks and best-practices.

1.2 Problem description and research questions

The thesis seeks to investigate and understand how aligned Norwegian hospitals are with well-known cybersecurity frameworks when it comes to cybersecurity considerations in the procurement process of digital medical equipment. Implementing security controls that enable you to take the right precautions can contribute to elevating the security posture of an organization, which in turn can aid in increasing resilience and reducing the potential attack-surface. Additionally, the thesis will comment on any potential improvements that could be done in the procurement process at Norwegian hospitals today, if applicable.

The problem statement for this Master thesis is to investigate how aligned Norwegian hospitals are with well-known cybersecurity frameworks when it comes to cybersecurity considerations in the procurement process of digital medical equipment.

The problem statement has three underlying research questions, which seeks to unveil which cybersecurity considerations that should be taken according to well-known frameworks, which cybersecurity considerations that are taken, and finally, if there are room for improvement in the current practice:

1. Which cybersecurity considerations is recommended to be taken in the procurement process of digital equipment, according to well-known frameworks and best practices?
2. Which cybersecurity considerations are taken at Norwegian hospitals in the procurement process of digital medical equipment today?
3. How could the current procurement practice of digital medical equipment at Norwegian hospitals be improved when it comes to cybersecurity?

The goal of research question number 1 is to summarize cybersecurity controls and considerations that should be taken in the procurement process of digital equipment. By compiling a list of recommended cybersecurity controls, we can say something regarding how things *should* be. This research question will be answered through a literature study.

Research question number 2 investigates what the current practice is at Norwegian hospitals, by interviewing those involved in the procurement process of digital medical equipment at different health regions in Norway. The results of these interviews contribute to saying something regarding how things generally are.

These two research questions will create two pillars of knowledge – how things should be versus how things are. The final research question will therefore discuss the potential gap, and any improvements that could be made to the current practice.

1.3 Limitations

The problem statement and research questions of the master thesis is comprehensive, hence there are some limitations to be able to handle with the timeframe and deadlines. Even though the thesis is about which cybersecurity considerations that are taken in the procurement process of digital medical equipment at Norwegian hospitals today, mainly public hospitals have been chosen to provide general findings regarding the subject.

1.4 Structure of this report

This thesis is divided into the following chapters:

- **Chapter 1 – Introduction**
  This chapter provides the reader with the theme of the thesis, background and purpose. The problem statement and research questions are presented, in addition to limitations of the thesis.

- **Chapter 2 – Theory**
  This chapter includes the theoretic framework for the thesis, where relevant literature is presented. This chapter provides the reader with knowledge about the relationship between cybersecurity and cybercrime, how cybercrime can affect hospitals, information regarding cybersecurity at Norwegian hospitals, recommended considerations, and requirements in the procurement process of digital medical equipment, and former research on cybersecurity in the procurement process. The theory creates the foundation for the discussion and conclusion later in this thesis.

- **Chapter 3 – Research method**
  This chapter describes the research method used in this thesis, such as the research design, case context and data collection, data reliability, credibility, and validity, and analytical approach.

- **Chapter 4 – Results**
  This chapter presents the results from the interviews that were conducted as part of this thesis. The interview questions are used as subheadings, where the answers from the interview participants are compiled. Finally, the findings are summarized at the end of the chapter.

- **Chapter 5 – Discussion**
  This chapter looks at the results from the interviews and discusses them in regard to the theoretical framework from chapter 2 and the research questions presented in chapter 1. Finally, there is a summary of the discussion and a disclaimer.

- **Chapter 6 – Conclusion**
  In the final chapter, the conclusion is presented, and the problem statement answered through answering the research questions. Additionally, the chapter contains recommendations to the health sector, and recommendations for further research.

2 Theory

This chapter includes the theoretic framework for the thesis, where relevant literature is presented. This chapter provides the reader with knowledge about the relationship between cybersecurity and cybercrime, how cybercrime can affect hospitals, information regarding cybersecurity at Norwegian hospitals, recommended considerations, and requirements in the procurement process of digital medical equipment, and former research on cybersecurity in the procurement process. The theory creates the foundation for the discussion and conclusion later in this thesis.

2.1 Introduction to cybersecurity

To understand the importance of the relationship between cyber and security, we can first look to the military and the domains which they operate in. Initially, the military were made up of two domains – the ground troops and sea. Then, aviation changed the game when the airplane was introduced, and air travel became a possibility. A new game changer came during the 1900's, when space was added as the fourth domain of operation, with satellite technology. It would take many years, but finally the fifth domain of operation was included, when the US Department of Defense, and NATO declared that cyber was a domain of war, placing it alongside the traditional battlegrounds (US Department of Defense, 2011) (NATO, 2021) (Evans, 2016).

Then there is information, which is more important than ever. Information contributes tremendously to decision-making processes, and effective operations in all layers of society (Kaye, 1995). Information has become big business, with companies like Facebook, Google, and Amazon collecting and processing information about every one of us daily. Consequently, there is a rising concern for privacy, due to the amount of personal data that is collected. Information put together can reveal a lot, which was seen at the American retail store Target in 2012: to try and hook expecting parents and make them loyal to the store, Target collected a lot of information to track their customers, among them the amount of unscented lotion women was buying. This item was more often bought by expecting women, usually at the beginning of their second trimester. Additionally, Target identified that pregnant women bought a lot of zinc, magnesium, and calcium. Altogether, Target identified 25 products, that when analyzed together, could help assign each customer a "pregnancy prediction" score, and estimation of the customer's due date. By doing this, they could start sending targeted ads and coupons to the customer. The story even reveals that an angry man entered a Target store, demanding to talk to a manager due to his daughter receiving coupons for maternity clothing, nursery furniture, and so on. The manager apologized and called the customer to apologize again a few days later, only to learn that the daughter in fact was expecting but had not told her father (Hill, 2012).

In this story, the customer received benefits from this data collection in form of coupons she could use, and even though it sounds like it is a violation of privacy, Target was on the right side of the law. The point of the story is that information put together can become a very powerful tool. Now imagine cyber criminals collecting various data unknowingly to their victim, to use either to blackmail, sabotage, or steal – some of this information might be publicly available, like a phone number, address, or email, while other information might be very personal, like medical records. In 2014, Reuters published an article that FBI warned healthcare providers to protect themselves against cyberattacks, after a large attack against Community Health Systems Inc. where personal information of 4.5 million patients were stolen. One of the reasons that the medical records were targeted, was that stolen health credentials could go for around $10 each, which, at the time, was around 10-20 times the value of a credit card number (Humer and Finkle, 2014). Stolen information like this can be used in a number of ways, all the way from keeping the data ransom (Gatlan, 2020) and thus disrupt normal operations, to blackmailing patients by threatening to publish medical therapy records online (Sipilä, 2020). According to the Norwegian National Security Authority, there is no sign of reduction in the threat landscape (Nasjonal Sikkerhetsmyndighet, 2022), and the actions performed by cybercriminals are getting more complex and comprehensive.

Cybersecurity exists on different levels, and in different areas. With reference to the military looking at cyber as the fifth domain of operation, we can say that cybersecurity exists on three different levels: strategic, tactical, and operational (White, 2009).

On the strategic level, a strategy for cybersecurity is developed, which contains security policies, how security should be organized in the organization, and how to evaluate and mitigate risks and threats. The tactical level is concerned with implementing systems that adhere to the security requirements and policies, while the operational level involves maintaining and monitoring the compliance of the cybersecurity policies and requirements. For cybersecurity to work and be taken seriously, it needs to be implemented using a top-down approach, where the senior management are involved in developing the organizational cybersecurity strategy.

2.2 Cybercrime

There is no common explanation for the term *cybercrime*, rather it is up to the different countries to define the scope of cybercrime themselves. However, many countries take as their starting point the criminal offenses described in the 2001 Council of Europe Convention on Cybercrime (Schjølberg, 2017). What is understood as cybercrime in Norway is today in accordance with the crime that deals with the protection of data in the Criminal Code of 2005. Cybercrime includes, among other things, data breaches, unjustified handling of access data, privacy violations, danger of service disruption, hacking of infrastructure, electronical document forgery, and so on.

There are several challenges when it comes to handling cybercrime in Norway: Norway is one of the most digitized countries in the world, and increased digitization means increased vulnerability in cyberspace. Additionally, there is a growing lack of expertise in Norway: according to a report from NIFU, it is assumed that there is a deficit of around 2000 cybersecurity experts today, and that this number will double by 2030 (Mark et al., 2017).

2.2.1 The cybercrime value chain model

Cyber-attacks might seem random to the untrained eye, and in some cases that might be true. The range of cybercriminals are huge, varying from bored irrational teenagers to nation-state threat actors. However, the larger and more serious cyber-criminal groups use a lot of time and resources in advance of an attack. Activities might include identifying possible victims, gathering information these victims, and planning the attack in excruciating detail, before performing the attack. Much like regular enterprises identifying customers, the larger cyber-criminal groups have a business model, in which they use a value chain model to identify possible targets, where they calculate whether they should perform an attack or not. Researchers at Michigan Institute of Technology (MIT) have made a model to systematically understand the cyber-attack business and economy, called the cybercrime value chain model (Huang et al., 2018).

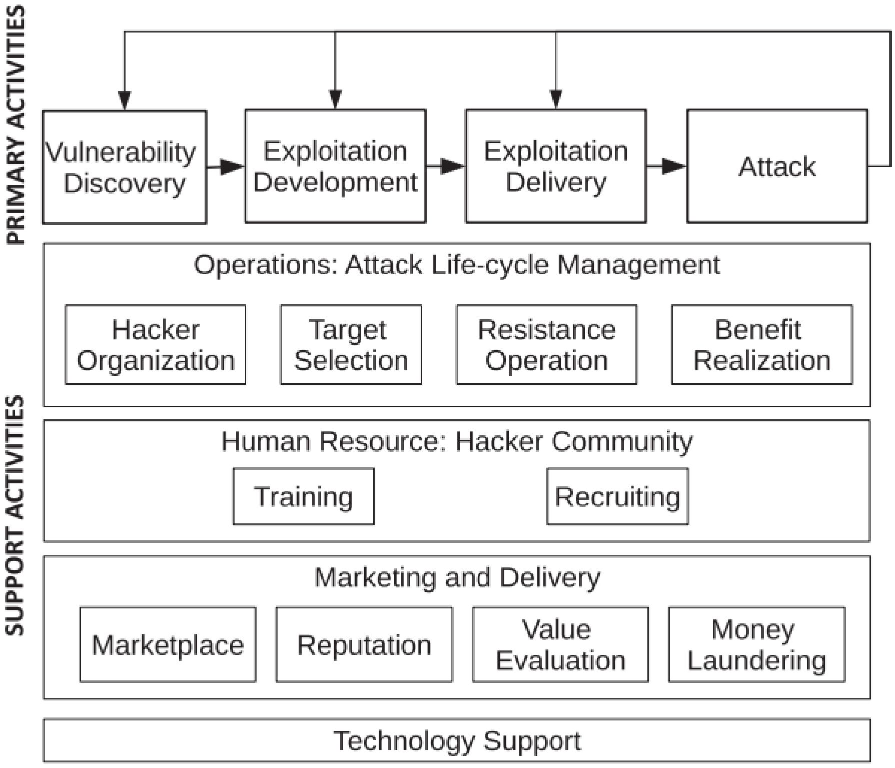

Figure 1; The cybercriminal value chain model that shows primary and supportive activities in a cybercriminal organization. Figure created by Huang et al. (2018)

This model explains all the underlying activities cybercriminals perform to ensure that they get the value they are after. Most importantly in this model, is an equation of the different areas, called the cyber-attack target selection rule:

$$P_e \times (B_{pm} + B_{pp}) \times E_r > C_{ps} + (P_a \times P_c \times C_c) + (C_{im} + C_{om})$$

The left side of the equation refers to the expected benefit of an attack, which includes:

- Ease of attack P_e: how easy will it be to conduct the attack and be successful
- Potential benefit B_p: which gains can the cyber-criminal make by performing the attack – this could be either monetary benefit (B_{pm}) or psychological benefit (B_{pp}).
- Ease of benefit realization E_r: after an attack, the result of the attack needs to be converted into tangible benefits, i.e., if information has been stolen, it needs to be sold – the more specific the information is, the harder it might be to sell it.

The right side of the equation refers to the expected cost of an attack, which includes:

- Psychological cost C_{ps}: this refers to the mental energy that needs to be expended during an attack, such as perseverance, fear of getting caught, and possible punishment.

- Expected penalty cost C_p: this cost captures the monetary opportunity costs of convicting the cyber-criminals, which are realized if a cyber-criminal actually gets arrested and convicted. The expected penalty cost consists of the arrest rate for the particular kind of cyber-attack P_a, the ease of the judicial process for convicting the cyber-criminal P_c, and the monetary opportunity cost is the cyber-criminal is convicted C_c.
- Operational costs C_o: these costs refer to the cost of carrying out a cyber-attack. To perform a cyber-attack, an investment needs to be made up-front (C_{im}), which includes hardware, software, services, time spent learning tools, searching for potential targets, and so on. Additionally, there is the monetary opportunity cost of the investment that should also be considered (C_{om})

Summarized, the expected benefit of an attack on the left side of the equation should outweigh the cost of an attack (operational cost + expected penalty cost) which is on the right side of the equation. Unfortunately, cyber-attacks do not necessarily consider borders of countries and continents, hence attacks can be performed from anywhere in the world. This results in an expected penalty costs being extremely low in certain circumstances, especially where attacks are performed by nation-states or by cyber-criminal organizations sponsored by nation-states. Consequently, the expected benefit often outweighs the expected costs, greenlighting too many cyber-attacks.

2.3 Cybersecurity events in hospitals

Throughout history, measures have been put in place to protect those in need, like children, elderly, wounded, and a like. In ancient Ireland, *Lex Innocentium* was a law of war that was designed to protect women, children, and other non-arms-bearing people in times of conflict (Houlihan, 2019). Traditionally, it has also been an unwritten rule not to attack institutions such as hospitals. However, over time that has changed in terms of cyberattacks, which has been seen on multiple occasions worldwide over the recent years.

On the 12th of May 2017, The National Health Services (NHS) in the UK was affected by a ransomware malware called WannaCry, in a rather unfortunate untargeted attack. The WannaCry malware exploited a vulnerability in Microsoft Windows and was unique in the sense that it had worm-like properties, which made it spread itself. The result was a worldwide infection, of over 200 000 computers in over 150 countries. For NHS, at least 80 of the 236 health trusts were affected by the malware, totaling the costs of the attack to £92 million (Acronis, 2020).

On the 27th of September 2020, Universal Health Service (abbreviated UHS), which is a Fortune 500 hospital in the USA with over 90000 employees and 3,5 million patients yearly (Gatlan, 2021), was attacked. The consequences of the attack was that normal operations at the hospital got disrupted, in some cases resulting in nurses and doctors using pen and paper to keep track of what had to be done (Hope, 2020). In this incident, a ransomware named Ryuk was used to try to get the hospital to pay to unlock their files that had been rendered useless after being encrypted. It took UHS over a month to restore systems back to normal (Gatlan, 2020), and the financial implications was totaling $67 million (Gatlan, 2021).

There have also been incidents in Norway, like against the Southern and Eastern Norway Regional Health Authority in 2018. Not much is known about that attack, other than that abnormal activity was discovered on the 8th of January, which resulted in a task force consisting of the Norwegian National Security Authority, the National Criminal Investigation Service, the Norwegian Intelligence Service, and the Norwegian Police Security Service investigating and handling the incident. It was believed that the attack was to gather intelligence against Norway, however an attribution was never made and the authorities could neither confirm or deny that patient information was extracted (NorSIS, 2018). Another attack was observed against the communications system used in ambulances in Northern Norway on the 8th of April 2022, disrupting the communication system responsible for delivering valuable information to road and airborne ambulances (Rostad et al., 2022). An attribution for this attack has not been made at the time of writing this thesis.

2.4 Organization of Norwegian hospitals

The public hospitals in Norway are owned and operated by the government (Helse- og omsorgsdepartementet, 2021b). The Ministry of Health and Care Services are responsible for operating public hospitals, thus providing good and equal health and care services to the population of Norway.

Norwegian hospitals are organized into four health regions, being the Northern, Western, South-Eastern and Central Norway Regional Health Authority. All these regions have their own IT departments, that are taking various degrees of responsibility for the ICT equipment in their respective region. Additionally, these four health regions own Sykehusinnkjøp, which is an organization heavily involved in the procurement process of different health related equipment, including medical technical equipment (Sykehusinnkjøp, 2022). Sykehusinnkjøp is responsible for procuring equipment in a responsible way, which includes ethical and environmental-friendly trade. Each year, Sykehusinnkjøp releases an assignment document, stating general guidelines, financial frameworks, and professional priorities for their involvement in the procurement process. In 2021, one of the three main goals was to increase quality and patient security, which according to Sykehusinnkjøp, entails that all procurement projects must include the sufficient information security competence to safeguard that adequate security requirements are included in assignment announcements, and throughout the negotiations with vendors (Sykehusinnkjøp, 2021). According to the assignment document, the information security communities in the health regions should be used for this.

There are also privately owned healthcare institutions in Norway, however, these hospitals also need to adhere to laws, regulations, and standards set by the government. This paper will focus primarily on public hospitals but include input from a hospital that is privately owned to widen the data collection and scope of the thesis, and thus substantiate the conclusion at the end of this paper.

2.5 Cybersecurity at Norwegian hospitals

2.5.1 NOU 2015: 13 – Digital vulnerability – secure society

In Norway, the Norwegian government regularly releases official reports called NOU's. These reports are a result from working groups who report on different aspect of

Norwegian society and can be published either as an Official Norwegian Report (NOU), or as a regular report.

In 2015, the Norwegian Ministry of Justice and Public Security received a report regarding digital vulnerabilities, referred to as NOU 2015:13 – Digital vulnerability – secure society (Lysneutvalget, 2015). In this report, a selection of researchers (Lysneutvalget) reviewed the findings they had made in connection with the digitalization of the Norwegian society. Although productivity and innovation rapidly increased, the report concluded that in general, the Norwegian society had become more vulnerable and exposed to risk, due to the increased digitalization. Societal value chains were suddenly more prone to errors and attacks due to the digitization. The report continued with a set of recommendations, among them to strengthen the IT security competence in different sectors, such as the health sector.

NOU 2015:13 contains a chapter dedicated to healthcare, which is defined as part of critical societal functions. The major concerns are preservation of life; hence the availability of systems and proper emergency response is listed as top priorities. Digital medical equipment is mentioned as something that has been seen as a rising trend in private homes, and while such equipment could relieve hospitals of some work, the report mentions that the reliability of that equipment might vary. Additionally, the complexity of the infrastructure will increase, and consequently the number of vulnerabilities.

Most importantly, the report mentions that "there are big differences between the regional healthcare institutions when it comes to solutions and technology, and there is no common process for coordination of vendor requirements". Additionally, the report says that small and medium sized healthcare institutions do not have the necessary resources to develop and implement information security management systems, which is an important part of the cybersecurity foundation in an organization.

Although the report is very focused towards maintaining the availability of data, it is also concerned with the confidentiality of the information and the privacy of the users. One of the major concerns mentioned in the healthcare chapter, is the uncontrolled harvest and processing of personal information, that both private citizens and hospitals might be unaware of. The report states that even though the digitalization might provide better privacy, many IT systems has inadequate security controls when it comes to the privacy of the users, and that healthcare personnel often gets excessive amount of access.

The report is summarized with a set of recommendations, where the first one touches on the need for stronger cybersecurity governance on a national level, which could impact the procurement process:

- **Stronger cybersecurity governance from the Ministry of Health and Care Services**
  The committee identified a need for stronger national management to identify and strengthen common needs and to avoid divergent solutions in the regions.
- **More research on ICT security in new health and welfare technology**
- **Establish solutions to meet developments in health and welfare technology**
- **Carry out several ICT exercises where critical systems are out of order**

2.5.2 Norwegian Government Meld. St. 38 (2016-2017)

As a response to the NOU 2015:13 report from Lysneutvalget, the Norwegian Government released a report one year later addressing some of the findings (Det Kongelige Justis- og Beredskapsdepartement, 2016). This was the first governmental white paper regarding IT security in Norway and provided an overview of the status of the follow-ups of the recommendations from Lysneutvalget.

Chapter 6.4 in Meld. St. 38 regarded outsourcing and pointed out that outsourcing could provide organizations with better security, provided that the organization was aware of the values that they were exposing during outsourcing, so that they could implement necessary measures.

The white paper does not mention the procurement process specifically, but rather the outsourcing process in general, and why it is important that organizations are aware of different IT (security) recommendations when outsourcing services. Additionally, the report mentions that the Norwegian health services are dependent on the private sector when it comes to services and solutions, and that the Minister of Healthcare will look at how information security should be handled when using private contractors in the healthcare sector.

Additionally, it addresses the recommendations mentioned by Lysneutvalget, and when it comes to the *stronger cybersecurity governance from the Ministry of Health and Care Services*, the current status at the time was that the Directorate of E-health was established from January 1st, 2016, to improve cybersecurity governance and coordination in e-health.

2.5.3 Code of Conduct for information security and data protection in the healthcare and care services sector: The Norm

In Norway, the Directorate of E-health is a subordinate institution of the Norwegian ministry of health and care services. The Directorate of E-health was established in 2016, tasked with the responsibility of steering and coordinating e-health in Norway across regions, local authorities, technical organizations, and other parties. Their main responsibility includes developing and implementing policies related to e-health, establishing standards, and administrating the use of e-health nationwide.

One of the tools/guidelines that the Directorate of E-health has released, is the Code of Conduct for information security and data protection in the healthcare and care services sector. This is quite a mouthful, so in Norwegian, it has been baptized The *Norm* (Direktoratet for e-helse, 2020). This is an information security policy that has a set of requirements that Norwegian health care institutions must adhere to, since it is quite close (and sometimes more stringent) than Norwegian law.

The latest version at the time of writing, is version 6.0, which was released on the 5th of February 2020. The document is divided into four areas, each covering different subareas that considers a multitude of different information security aspects. The four main areas are *Governance and responsibility*, *Risk management*, *Basic rules for processing of health and patient information*, and *Information security*. Summarized, there are 294 requirements, where the majority of them has a link to ISO 27001.

One of the requirements (number 181) mentions medical equipment (not medical *technical* equipment specifically) and has a checkpoint for whether medical equipment is included in the organization’s work on information security.

Other requirements in *The Norm* considers the procurement process, specifically requirement 244, 264, 265, and 268:

Table 1; Requirements from the Norm in the procurement process

Number	Requirement	Chapter in the Norm	Reference to ISO 27001
244	When outsourcing ICT functions or other functions of importance for information security or privacy, the agreement shall at least include the following points related to information security and privacy: • Documented risk assessment that shows that the service-outsourcing company's level of acceptable risk and the Norm's security level have been established. When outsourcing ICT services to other countries, conditions at the host country should be considered because they may affect the risk assessment. • Which tasks of safety significance are covered, and the responsibilities for these • Description of the supplier's solution and interface to the business in the form of configuration maps	5.7.3	A.15.1.2
264	Are procurements, vendor follow-up and vendor management included in the company's management system for information security? All phases in vendor management, from procurement to the conclusion of the agreement, must be covered.	5.7.7	A.15.1
265	Does the organization ensure vendor follow-up by: • clarifying responsibilities and roles • including competent information security and privacy resources in the procurement and vendor management • including the company's management (and the board if relevant) in decisions concerning the use of private vendors and/or the outsourcing of services of a certain size	5.7.7	A.15.1 A.6.1.1 7.2 5.1
268	Is it ensured that relevant security requirements are included in all procurements?	5.7.7	A.14.1.1

2.5.3.1 Privacy and information security – medical technical equipment

In June 2021, a supporting document for medical technical equipment was released in version 2.0. This goal of this document is to raise the understanding of the requirements and approach to information security for Norwegian hospitals and their vendors. The document includes both recommendations, such as using vendors that do not process health records, and requirements, such as reference to the requirements from the Norm (relevant requirements mentioned in the section above).

The document contains a chapter dedicated to the procurement process of medical equipment, and which information security requirements that should be adhered to (chapter 3.8.1 in that document). This chapter refers both to requirements from the Norm, and a recommendation to consult the Medical Device Coordination Group (MDCG) 2019-16 Guidance on Cybersecurity for medical devices (European Commission, 2020). The supportive document recommends consulting MDCG 2019-16 to include appropriate vendor requirements. It additionally recommends to consult the American Food and Drug Administration (FDA) for network connected medical equipment (Food and Drug Administration, 2014), so that hospitals can request for information on whether the vendors adhere to these principles or not (documentation, access control, and similar).

Finally, the document also states that all procurement should be conducted in close cooperation between medical-technical departments and the clinic. The law and regulations on the handling of medical equipment require that the equipment must be assessed by users and technical personnel for the intended area before the procurement can be completed (Lovdata, 2014). A purchaser should therefore never acquire any equipment without this being professionally cleared by the user and medical technical departments.

2.5.4 Observations from the Office of the Auditor General

The office of the Auditor General (OAG) (Riksrevisjonen, 2022) has made several investigations into the cyber and information security posture at Norwegian hospitals and healthcare institutions. This chapter will highlight the findings from two of them, performed in 2015 and 2020 respectively.

2.5.4.1 Investigation of the health institutions' handling of information security in medical-technical equipment

In 2015, OAG released a report on findings from their investigation of the health institutions' handling of information security in medical-technical equipment (Riksrevisjonen, 2015).

The goal of the audit was to investigate whether Norwegian hospitals had adequate information security when using medical-technical equipment. The audit included a document analysis of 19 Norwegian hospitals, in addition to 6 interviews. One of the key findings of the audit was that Norwegian hospitals does not set sufficient requirements for information security in agreements with vendors of medical-technical equipment, in addition to inadequate follow-up of vendors. OAG found that only 6 out of the 19 hospitals had some sort of requirements regarding information security, and that the vendors usually wrote the agreements. Additionally, there was very limited cooperation between hospitals when dealing with vendors. All the interviewed hospitals mentioned the importance of having information security requirements in the requirement specification, and that cooperation between hospitals and health regions should be established to enable the hospitals to influence the vendors when it comes to information security.

OAG also revealed that none of the 19 hospitals had documented any security audits, control checks, or follow-up of any of the vendors during the last year. This entails that the hospitals have no knowledge regarding the vendors work on information security challenges. Only two of the 19 hospitals had documented that a risk and vulnerability analysis had been conducted on the information security in medical-technical equipment. Furthermore, the information OAG received, showed that there was no common template for conducting a risk and vulnerability analysis. The risk and vulnerability analyses that were usually conducted, was more about patient safety and the technical side, rather than the information security. One of the mentioned challenges, was that even smaller hospitals had to do the same risk and vulnerability analyses since they were using the same type of equipment, however, they did not have the manpower to conduct these analyses.

When it came to organization, OAG found out that it was the nurses and doctors that used the equipment, IT was responsible for connectivity, and that the medical-technical department was responsible for procurement, operation, and maintenance. When it came to the procurement process, some of the equipment were bought regionally, and some directly by the hospital. At the time, the hospital's procurement service (HINAS), which was owned by the regional hospitals to do purchases, were not very involved in the procurement process of medical-technical equipment.

Summarized, only one third of the hospitals had some sort of requirements for the vendors' processing of personal identifiable information (PII). OAG suggested that these requirements could include software updates and equipment maintenance, how the vendors should process PII's, and how the vendors should implement security controls to safeguard the confidentiality, integrity, and availability of the collected data. More often than not, it was the vendors that wrote the agreements, and information security was often not even mentioned. Even though the regional IT-department had prepared information security guidelines, these were rarely used to set requirements for vendors. None of the hospitals did any audits or controls of the vendors, even though they had the right and opportunity to do so. Risk and vulnerability analyses was also very limited, and only two out of the 19 hospitals had performed one regarding an individual medical-technical equipment. It became clear to OAG that the regional health trusts and the hospitals had different views on the information security requirements that should be set for vendors.

Summarized, the report states that the hospitals do not set sufficient requirements for information security in their vendor agreements of medical technical equipment, in addition to having inadequate follow-up of the vendors. The hospitals also have inadequate overview of risks associated with information security in medical technical equipment, and there are unclear lines of responsibility internally in the hospitals and between hospitals and the regional ICT departments. Based on this, the OAG recommends that the Ministry of Health and Care Services ensures that the health regions and hospitals comply with current laws and regulations for information security and privacy, that the health regions ensure better coordination between regions and between hospitals internally in their region, that requirements for information security in medical technical equipment becomes more uniform, and that laws and regulations are followed by setting clear vendor requirements in the agreements.

2.5.4.2 Investigation of the health institutions' prevention of attacks on the ICT systems

Another report was released by the OAG in December 2020 (Riksrevisjonen, 2020). In this report, the OAG investigated to what extent Norwegian health institutions was working to prevent attacks on their ICT systems. The results highlighted in the report, showed that the situation was highly reprehensible.

Chapter 6.4.2 of the report deals with ambiguities in the responsibility for safeguarding the security of medical technical equipment. Referring to the report from 2015 (see chapter 2.4.4.1), the OAG concluded that there still were ambiguities in the information security responsibility five years later. Among the challenges the OAG identified, were the regional management systems inability to address and determine how information security in medical technical equipment should be handled, which role the medical technical departments in the hospitals should play, and how to distribute the information security management responsibility across the hospitals, health regions, and ICT vendors. Additionally, there were insufficient mentioning of how the hospitals should adhere to requirements regarding secure on-prem operations of medical technical equipment.

One of the other findings from the OAG were the challenges in terms of acquiring security updates for older equipment. Some equipment had reached end of support, which means that the vendor no longer provides security updates, while other equipment was prone to error when upgrading, which could trigger hazards to patient safety. One major discovery was that medical technical equipment usually suffered from low security maturity, where the equipment often lacked security update functions, end-point security, logging, and access management. Even large vendors did not adhere to Microsoft's update schedules.

The OAG also repeats the need for greater demands against vendors in the procurement process, to force vendors to implement information security in the systems and equipment they deliver. According to an interview done by the OAG with HelseCERT (Norwegian Health Cyber Emergency Response Team), there are signs that this is starting to happen.

Another challenge that is mentioned is the balance-act of using secure equipment, while safeguarding patient treatment – it is more important to treat the patient, rather than to safeguard the confidentiality, integrity, or availability of data. However, the long-term challenges might be significant if adequate information security requirements are not set and met. Different priorities also pose a challenge since vendors and hospitals sometimes have different focus when it comes to certain equipment properties.

Room for improvement was identified when it came to the role that Sykehusinnkjøp has: the audit revealed that when the organization was founded, it was not assigned information security responsibility, neither to coordinate requirements, nor to set specific information security requirements for the procurement process. At the time, there was no dedicated information security roles, other than a privacy officer responsible for Sykehusinnkjøp itself. Due to the inadequate competence, Sykehusinnkjøp is reliant on information security competence being provided by the health regions themselves, which often constituted a challenge. In interviews, Sykehusinnkjøp admitted that there was not established structures to strengthen information security in the national procurement. Additionally, risk and vulnerability analyses were handled differently across the health regions, which seems to be a "hang-up" from the past. Nonetheless, according to HEMIT

(Central Norway Regional Health Authority's IT department), the report from the OAG led to an increased focus on strengthening their ICT systems, https://hemit.no/nyheter/ikt-sikkerheten-ma-bli-bedre and in the report from the OAG, it is mentioned that Sykehusinnkjøp and HEMIT cooperates by going through the procurement plan and identifying projects in need of greater information security focus. As a measure to increase the information security awareness in the procurement process of medical technical equipment, a fact sheet has also been made (there is no reference to where this document can be found in the report from the OAG).

The report concludes with recommendations to the different stakeholders involved, hereunder the hospitals, the health regions, and the Ministry of Health and Care Services:

Hospitals:

- Clarify roles and responsibilities
- Increased security behavior in ICT department and clinical personnel
- Necessary technical security measures are implemented
- Systematic clean up in old solutions and sensitive health and personal information

Regional level:

- The health regions must ensure that cybersecurity requirements set for the health regions are followed up, so that the necessary progress is achieved in the improvement work.
- They must ensure that the necessary technical security measures are implemented based on recognized security principles that ensure an acceptable level of security in line with legal requirements.
- They must take greater responsibility for coordinating information security work in their own region, and, among other things, make the necessary clarifications about responsibilities, roles, and tasks.
- They should consider appropriate measures for increased cooperation across the health regions to strengthen information security in the sector.

Ministry of Health and Care services:

- Whether the Directorate for e-Health should have a clearer role when it comes to information security.

2.6 Digital medical technical equipment

Digital medical technical equipment referred to in this paper, refers to equipment used in Norwegian hospitals to diagnose, prevent, monitor, treat, or relieve illness, injury, or handicap in humans that in some ways are connected to the network (Helse- og omsorgsdepartementet, 2021a). The equipment is also referred to as electro medical equipment, and more recently just medical equipment.

Examples of digital medical technical equipment are blood pressure monitors, ultrasound, x-ray, respirators, hearth rate monitors, laboratory equipment, CT, and MR scan machines (St. Olavs Hospital, 2022).

Digital medical technical equipment plays an increasingly important part in Norwegian hospitals as we continue to develop new, more efficient ways to treat patients, and the availability of such equipment can be the difference between life and death.

Some medical equipment is categorized as IVD equipment. IVD is an abbreviation of In Vitro Diagnostic medical devices, where "in vitro" is Latin for "in glass" (Otterholt, 2021), meaning that IVD is a sort of medical device that operates outside the human body, usually laboratory equipment with reagent glass.

IVD equipment has been regulated by the EU since 1993 but was updated with the IVD Regulation (IVDR) in 2017 (Hall and Payne, 2018). This new regulation requires vendors to develop and manufacture their product in accordance with the state of the art, which includes information and cyber security measurements, risk management principles, etc., to stay up to date in relation to the current time and threat landscape (Deuschler, 2020).

2.7 Recommended security controls, considerations, and practices in the procurement phase

To provide a list of recommended cybersecurity considerations that should be taken in the procurement process, a set of well-known frameworks and best practices have been compared. These are as follow:

- NIST 800-53 (National Institute for Standards and Technology, 2020)
- ISO/IEC 27001 (ISMS.online, 2020)
- CIS controls (Center for Internet Security, 2019)
- COBIT 2019 (ISACA, 2018)
- ISF Standard of Good Practice (Information Security Forum, 2021),
- The Norwegian National Security Authority (NSM) (Norwegian National Security Authority, 2020)

Although IoT devices for the consumer market are not directly comparable to digital medical equipment due to digital medical equipment being way more regulated, the considerations taken in the procurement phase should at least be similar.

During the examination of the different frameworks, it became evident that not all these frameworks considered the procurement phase in the device lifecycle. Only NIST, COBIT, CIS, ISF, and NSM referenced security controls for the procurement phase, and of these five, there were only three that had adequate levels of detail to be usable to establish a foundation for necessary cybersecurity considerations that should be taken in the procurement process of digital equipment.

These were the NIST800-53, ISF Standard of Good Practice, and the Norwegian National Security Authority Basic Principles for ICT Security, which will be summarized here. Additionally, the controls from COBIT and CIS will be mentioned.

2.7.1 NIST 800-53

The NIST 800-53 framework consists of 1189 controls divided into 20 categories. The controls are divided into base controls and control enhancements, which can be used to strengthen the related base control by adding specificity to it (National Institute for Standards and Technology, 2020).

NIST 800-53 contains a family of controls called System and Services Acquisition, which is abbreviated SA. SA-4 proved to be specifically appropriate for the procurement process:

Table 2; Relevant cybersecurity considerations in the procurement process according to the NIST 800-53 framework

Reference to framework control ID	Base control description	Control enhancement description
SA-4	Include the following requirements, descriptions, and criteria, explicitly or by reference, using standardized contract language and/or organization-defined contract language, in the acquisition contract for the system, component or service: a) security and privacy functional requirements, b) strength of mechanism requirements, c) security and privacy assurance requirements, d) controls needed to satisfy the security and privacy requirements, e) security and privacy documentation requirements, f) requirements for protecting security and privacy documentation, g) description of the system development environment, and environment in which the system is intended to operate, h) allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management, and i) acceptance criteria	1) Functional properties of controls: Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented

Summarized, the NIST 800-53 framework recommends that a procurement contract is made in advance before purchasing the equipment. This contract should include nine different requirements, descriptions, and criteria, to safeguard that the vendor produces a safe and secure product or service.

2.7.2 ISF Standard of Good Practice

The Internet Security Forum (ISF) has released a framework called Standard of Good Practice (Information Security Forum, 2021), that consists of 4000+ questions that can be used to measure cybersecurity maturity. These questions are divided into different areas within information and communications technology, ranging from infrastructure, to process, to people, and strategy. Additionally, the framework references other frameworks such as ISO27001, CIS and COBIT 2019.

When it comes to cybersecurity considerations that should be taken in the procurement process, the Standard of Good Practice offers very detailed descriptions, and like NIST 800-53, the controls are divided into different areas. For the procurement phase, the recommended cybersecurity controls are in the chapter describing Physical Asset Management controls, abbreviated PA.

Table 3; Relevant cybersecurity considerations in the procurement process according to the ISF Standard of Good Practice framework

Framework control ID reference	Control heading	Control description
PA.1.1 and subcategories PA.1.1.1 PA.1.1.1a PA.1.1.1c PA.1.1.1d PA.1.1.1e PA.1.1.1f	**Hardware lifecycle management: There should be documented standards/procedures for managing the lifecycle of hardware, which cover:**	a) guidelines for selecting hardware (e.g. lists of approved suppliers, security considerations and contractual terms) c) a process for reviewing and approving hardware prior to acquisition d) categorization of hardware, based on the type and classification of information processed, stored, and transmitted e) maintaining a record of hardware in a register f) tracking hardware throughout its lifecycle
PA.1.1.2j	**Standards/procedures should apply to all hardware acquired throughout the organization, including:**	j) specialist devices such as medical equipment
PA.1.1.4a PA.1.1.4b PA.1.1.4c	**Hardware should be:**	a) acquired from approved suppliers, preferably those with a proven record of providing robust and resilient equipment b) tested prior to use to help identify and resolve security weaknesses c) supported by maintenance arrangements.

PA.1.1.5a **PA.1.1.5b** **PA.1.1.5c** **PA.1.1.5d** **PA.1.1.5e**	**When acquiring hardware:**	a) security requirements should be identified b) suppliers should demonstrate that they can meet security requirements c) a high priority should be placed on reliability in the selection process d) contractual terms should include security requirements and be agreed with suppliers e) warranty and maintenance constraints should be clarified and agreed to avoid issues relating to the implementation of security controls.
PA.1.1.6	**Assurance should be obtained from suppliers/manufacturers about the level of security provided by their products for example by**	Producing results of security-related tests, vulnerability assessments and adherence to technical standards.
PA.1.1.7a **PA.1.1.7b**	**The risk of potential security weaknesses in hardware should be reduced by:**	a) obtaining and reviewing external assessments from trusted sources b) identifying security deficiencies (e.g., by detailed inspection, vulnerability scanning, reference to published sources or by participating in user/discussion groups)
PA.1.1.8	**The acquisition of hardware should be reviewed by individuals who have the necessary skills to evaluate associated information security requirements and be subject to approval by an appropriate business manager.**	The acquisition of hardware should be reviewed by individuals who have the necessary skills to evaluate associated information security requirements and be subject to approval by an appropriate business manager.

Summarized, the Standard of Good Practice is a very thorough framework that considers a lot of different aspects of the procurement process, consisting of 18 different recommendations.

2.7.3 The Norwegian National Security Authority Basic Principles for ICT Security

Finally, we have the Basic Principles for ICT Security (Norwegian National Security Authority, 2020), which is a set of recommendations released by the Norwegian National

Security Authority (NSM). This is a public framework, available for anyone that need guidance on implementing the basic security controls necessary to safeguard their organization.

Table 4; Relevant cybersecurity considerations in the procurement process according to the NSM Basic Principles for ICT Security framework

Framework control ID reference	Control heading	Control description
1.2.2	**Determine guidelines for approved devices and software in the organization**	A) The organization should decide i) what kind of devices and software the users need, ii) What kind of devices and software that is allowed, iii) What kind of devices and software that is forbidden, iv) How to handle this within the organization B) Prepare and maintain an overview of devices and software approved for use in the organization. C) Communicate guidelines to the employees, and description of purpose and legal use of devices and software.
2.1.1	**Integrate security into your organization's procurement process**	Establish requirements for ICT security when procuring all ICT products and ICT services. Include security throughout the life cycle from acquisition to disposal.
2.1.2	**Buy modern and updated hardware and software**	This should be done to make sure that security is built in. Additionally, one should make sure that: A) Only use devices that are supported with security updates from the vendor, B) To only procure devices that contain newer security functionality and protocols, C) That older legacy devices are phased out, D) Ask the vendor about risk and vulnerabilities where appropriate, and if there are any possibilities of hardening or elevated protection.
2.3.10	**Reduce IoT device risks**	A) Creating a plan for implementation of such devices, including security aspects with a risk assessment, including the cloud

		service the IoT device will communicate with B) Only buy IoT devices with built-in security functionality such as i) Ability to install security updates ii) Possibility to change standard passwords iii) Possibility to restrict communications to internal communication only C) Monitor device traffic D) Isolate devices into dedicated security zones using network segmentation or similar E) Carefully consider physical location of IoT devices so that unauthorized persons cannot gain physical access to the device.

Summarized, the Basic principles of ICT Security by the Norwegian National Security Authority contains four different control measures, consisting of several aspects that should be taken into consideration. The last control is guided towards IoT devices but are just as valid for digital medical equipment.

2.7.4 COBIT 2019 and CIS Controls

These two frameworks briefly touch on the procurement process as follows:

CIS: Ensure that only software applications or operating systems currently supported and receiving vendor updates are added to the organization’s authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system. This control is important to prevent buildup of technical debt and to prevent creating possible attack vectors for adversaries.

COBIT 2019: Procure all assets based on approved requests and in accordance with the enterprise procurement policies and practices.

Since these frameworks are limited when it comes to content regarding the procurement process, and the information they contain are similar to those three frameworks mentioned in the chapters above, they will not be mentioned throughout the rest of this thesis.

2.8 Former research on cybersecurity in the procurement process in hospitals

There have been some previous studies addressing the cybersecurity in medical devices and considerations that should be taken in the procurement process of such equipment. According to a study published in 2014, an effective device management plan starts at the procurement stage, where the hospitals should ensure that the device has good security features and that the vendor will provide continuing support (Coronado and Wong, 2014). A study from 2018 called *The Evolving State of Medical Device Cybersecurity* (Schwartz et al., 2018) mentions that it is the medical needs that drive device purchases, and that ideally, the IT or medical technical department are involved in the procurement process. However, limited cybersecurity awareness in the clinic or the absence of a procurement process could lead to insecure devices being procured. Another challenge mentioned by Schwartz et al., is the need for clear requirements, which often are absent as well, in addition to common frameworks or processes to assess levels of security risk. Schwartz et al. suggests that a minimum set of medical device cybersecurity requirements should be articulated across the device life cycle, including the procurement process. This will not only enable the hospitals to procure more secure equipment, but it will also create a common baseline that vendors can follow to manufacture equipment compliant to this baseline. This is backed by a research paper titled *Cybersecurity Expert: Medical Devices Have "A Long Way to Go"*, which also suggests that security requirements should be built into the procurement process, and that since there are a limited number of hospitals, the hospitals need to work together to show vendors that they take security seriously (Rios, 2015).

Another research paper published by the Delft University of Technology titled *The role of cybersecurity in hospital procurement processes: key factors* (Baren, 2021), recommends that the ENISA Procurement Guidelines for Cybersecurity in Hospitals are followed, since it is an aggregation of best practices (the first recommended practice in the ENISA Guideline is the involvement of the IT Department in the procurement process). The ENISA procurement process lifecycle for hospitals is summarized in the figure below (ENISA, 2020):

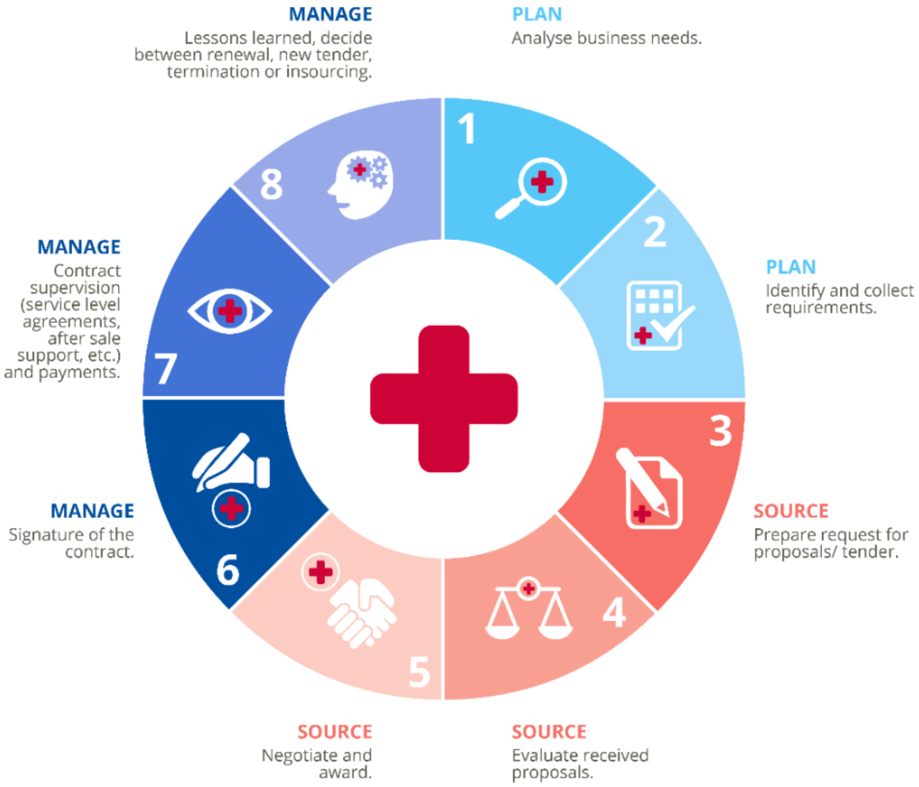
MANAGE
Lessons learned, decide between renewal, new tender, termination or insourcing.
PLAN
Analyse business needs.
MANAGE
Contract supervision (service level agreements, after sale support, etc.) and payments.
PLAN
Identify and collect requirements.
MANAGE
Signature of the contract.
SOURCE
Prepare request for proposals/ tender.
SOURCE
Negotiate and award.
SOURCE
Evaluate received proposals.
1
2
3
4
5
6
7
8

Figure 2; The ENISA Procurement process lifecycle for hospitals, developed by the European Union to highlight the different phases of the device lifecycle (ENISA, 2020).

3 Research method

This master's thesis investigates which cybersecurity considerations Norwegian hospitals take during the procurement phase of digital medical equipment. This chapter will explain how research was conducted and the research methods that were used to find answers to the research questions and problem statement.

3.1 Method design description

Research methods are guidelines that are used in scientific research (Grønmo, 2021). In the social sciences, the research methods comprise the systematic and methodical procedures used to establish reliable and valid theories about people in different societies. The research methods include principles and rules for areas such as theoretical discussion and argumentation, and techniques for planning and conducting empirical investigations.

Hence, the scientific method can be viewed as a strategy to gather empiricism with the purpose of producing valid and credible knowledge of reality (Jacobsen, 2015).

When researching a subject, we have a *theory* or *hypothesis* about something. Then, we gather information about what we experience as the *reality*. In the research community, this information is referred to as *empirical data* or, in other words, information about reality. Theory, empirical data, and reality are directly connected as shown in figure 1 below:

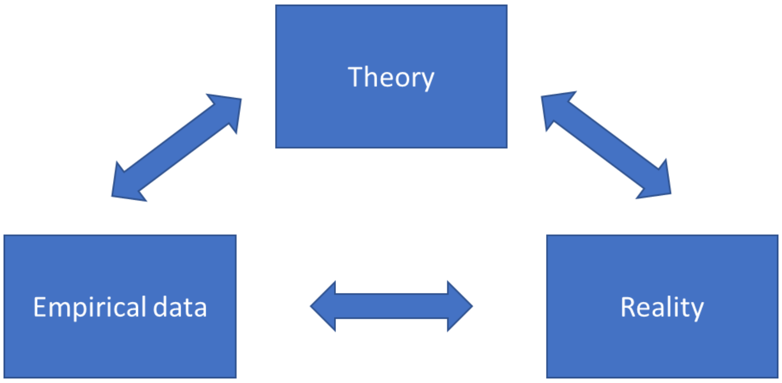

Figure 3; The figure shows the connection between theory, empirical data and reality as explained in the book "How to conduct surveys" by Dag Ingvar Jacobsen (Jacobsen, 2015)

The connection between theory and empirical data is what is known as the methods domain (Jacobsen, 2015). To be able to produce information about reality that is valid and credible, there is need for a systematic approach. Because of that, the scientific method constructs a hypothesis regarding the perception of reality, then formulates research questions that can answer the hypothesis, which in turn decides what kind of research method that should be used to collect information that can be used to either verify or falsify our perception of reality:

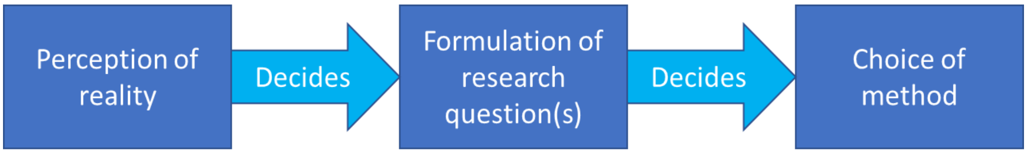

Figure 4; The figure shows how our perception of reality decides what kind of research method we should use (Jacobsen, 2015)

This chapter will start by addressing the challenges elucidating the problem statement and conducting surveys, in addition to sharing the thought process so that the reader will better understand the decision-making processes.

The stages in the research process will be explained, like how the participants got contacted, how the interviews were planned and conducted, and how information was collected.

This chapter closes out by discussing the validity and reliability of the data that that was collected, what the strengths and weaknesses are, in addition to which consequences this can have for the research and conclusion.

3.2 Phases in a research process

All research follows a set of relatively similar phases. In each of these phases, the researcher must make choices that will have consequences for the study's credibility and validity (Jacobsen, 2015). According to Jacobsen (2015), there are seven different phases that should be included in a research process:

- Developing a problem statement
- Choice of research design
- Choice of information type – qualitative or quantitative
- Choice of data collection
- Selection of units
- How to perform data analysis
- Evaluating how to interpret the results

3.2.1 Developing the problem statement

According to Jacobsen (Jacobsen, 2015), research can roughly be divided into two categories:

1. To describe the current situation as it is, also known as a descriptive and exploratory approach

2. To identify the effect of a phenomenon, for example if there is an increase in productivity after employees attend a training program. This is known as causal or explanatory approach.

The goal of this thesis is to describe the current situation; hence a descriptive and exploratory approach has been chosen when formulating the problem statement:

> *Which cybersecurity considerations are taken at Norwegian hospitals in the procurement phase of digital medical equipment?*

3.2.2 Research design: small *N*-case study

Research designs can be divided into either correlational (descriptive), or causal (Jacobsen, 2015), where the goal is to describe a situation and which conditions occur simultaneously. This research can be done by conducting a survey that investigates a cross section at a specific time.

Since the problem statement is grounded in a desire to describe the current situation, a case study has been chosen as the appropriate research design (Jacobsen, 2015). Common for case studies is that they are limited to space and time, which is aligned with the goal of finding out which cybersecurity considerations that are *currently* taken in the procurement process at *Norwegian* healthcare institutions when procuring digital medical equipment.

Units are often represented by the letter *N*, which is an abbreviation for *Numbers*. Small *N*-studies are characterized by only selecting a few units, which is suited for researching phenomena where there is a natural limit on unit selections, such as Norwegian hospitals (Jacobsen, 2015).

Therefore, the chosen research design can be described as a small *N*-case study.

3.2.3 Qualitative approach

To be able to describe reality, information needs to be gathered. Research to gather this information can be conducted in several ways, and information gathering can usually by divided into two main categories: quantitative or qualitative gathering of data. A quantitative approach is based on the premise that social reality can be measured using methods that provide information in the form of numbers. A qualitative approach on the other hand, is based on the premise that reality is too complex to be reduced to numbers, and that one must therefore collect information in the form of words that allow for more nuances (Jacobsen, 2015). It can be argued that a qualitative approach often is more suitable for clarifying an unresolved topic in more detail, and for producing a nuanced description of the topic (Jacobsen, 2015).

While a quantitative approach usually is used to seek explanations and overview, a qualitative approach highlights insights and seeks to understand a phenomenon (Tjora, 2020). There are rarely a strict quantitative or qualitative approach, but rather a combination of the two.

Nonetheless, in this thesis, the focus will be on gathering statements from Norwegian hospitals on *which* cybersecurity considerations they take in the procurement process of digital medical equipment. These statements will be gathered by performing interviews; hence, a qualitative approach will be used in this thesis.

Ontology, epistemology, and methodology

This thesis is composed of facts, but also of opinions and perceptions of reality. Consequently, it is appropriate to mention the terms ontology, epistemology, and methodology, and how they are intertwined.

The term *ontology* stems from ancient Greece and can be translated to "how things actually are" (Jacobsen, 2015). Ontology is thus the doctrine of what reality actually looks like. As seen repeatedly throughout history, it is often hard, or sometimes even impossible, to come to an agreed understanding of how reality actually is. In many instances, there is not a clear answer to whether one answer is correct rather than another, if you ask enough people. We say that different people have different ontologies, or in other words, perceptions of how things actually are.

Epistemology can be translated to something like "the doctrine of knowledge" and revolves around to what extent it is possible to obtain true knowledge of this world (Jacobsen, 2015). Epistemology is the acknowledgement that there is a difference between how reality actually is, and how reality is perceived by the researcher.

What this means for this thesis, is that units must be carefully selected before gathering information, so that the gap between reality and perceived reality is as small as possible. Consequently, the information must be gathered as close to the source as possible (i.e., those in charge of the procurement process), before answering the research questions. Additionally, it is important to be aware of the fact that the perception and understanding of the information that is gathered, might contain content, context, and connections that are not discovered. This leads us onto methodology, which are the techniques used to acquire knowledge about reality (Jacobsen, 2015). This thesis uses a holistic deductive approach, going from theory about a complex phenomenon to empiricism. In other words, this thesis comprises of a search for facts about a complex reality, guided by theoretical assumptions about said complex reality.

3.3 Data collection

According to Jacobsen (2015), there are four different forms of data collection in a qualitative study:

- Individual interviews
- Focus groups
- Observation
- Literature review

Initially in a data collection process, there is collection of primary data, where observation, individual interviews, and group interviews are the most common types. Then, there is collection of secondary data, which is referred to as source review.

3.3.1 Literature study

To shed additional light on the procurement process, research question 1 asks which cybersecurity considerations that *should* be taken in the procurement process of digital equipment, according to well-known frameworks and best practices. Including this research question enables this thesis to debate on the maturity of cybersecurity in the procurement phase in different Norwegian hospitals. To answer this question, a literature study will be performed, since this information is documented and available online.

A literature study can be used to summarize the knowledge within a research field or subject area. This knowledge can have the character of theory, empiricism, or method. Reading research literature provides new and relevant insight (Everett and Furseth, 2019). Additionally, it is a way of shielding the participants in a study by acquiring knowledge through literature, hence reducing the use of interview participants time (Tjora, 2020).

The use of documents as data material is central in most research projects. Documents are often used as *secondary data*, in other words they are used in addition to interviews and observations (Tjora, 2020). One thing to notice, is that literature on a phenomenon is written at a specific time and place, sometimes even with particular readers in mind. It is therefore paramount to put the literature in a context, and answer questions like *"when was the document written?"*, *"where was the document written, by whom and for what purpose?"* (Tjora, 2020).

A literature study is a great way to find out what people have said, done and researched previously, which can be built upon (Jacobsen, 2015). However, secondary data is often tailored to the purpose of the original data collector. It is therefore important to be aware of its limits, since units, values, and variables might not suit other research. Additionally, data is often transformed to tell a story or prove a point, while the raw data might not be available at all.

Finally, there is the question of how trustworthy the information in the literature is. In primary data collection (i.e., interviews), the researcher has a certain degree of control of the availability of data, since they have the backstory on how it was collected, analyzed, and used. By using secondary data, this control is often lost – we do not necessarily know how data was collected, which measurement methods that were used, data collection methods, and so on (Jacobsen, 2015).

With all this in mind, it is easier to mitigate the risk of gathering incorrect or misleading information, by scrutinizing the sources being used to gather said information. The following criteria has been taken into account (Jacobsen, 2015):

- Assessment of the source's origin and credibility
- Assessment of who is the recipient and sender of the information
- Knowledge and competence of the author
- Whether the source provides private or public information
- Assessment of website purpose, domain suffix and quality

The literature in this thesis has been gathered through a range of public and private sources, using private search engines like NTNU's private library database Oria, and public search engines like Google and Google Scholar. Additionally, searches have been conducted on governmental websites, and EU official sites. To build the foundation for the thesis and raise the readers awareness and understanding of how serious the potential cybersecurity threats are, news outlets and similar has also been used as sources.

All sources used in this thesis have been listed in the reference chapter at the end of this thesis.

The following search words have been used throughout this master thesis:

Table 5; Search words used to locate literature to use in this study

Theme	Search phrase
Procurement and acquisition	"Procurement process digital equipment" "Procurement cybersecurity" "Procurement medical equipment"
Medical devices	"Medical device cybersecurity" "Lifecycle management cybersecurity controls"

The sources used for the theory chapter 2.8 (former research on cybersecurity in the procurement process in hospitals) have all been from assessed journals found through NTNU's knowledge database Oria.

3.3.2 Interviews

To identify which cybersecurity considerations Norwegian hospitals' take in the procurement process of digital medical equipment, individual interviews are used to gather information. According to Jacobsen (2015), individual interviews are best suited when relatively few units will be investigated. In this case, there are several Norwegian hospitals, but many of them operates quite similarly and even cooperate closely. Additionally, there is an added interest in discovering potential differences in how the various hospitals operate when they acquire new digital equipment. This can be more easily discovered in a face-to-face interview, since stakeholders can elaborate on how they adhere to cybersecurity in the procurement process, which frameworks or best practices they follow and so on.

An interview can have different degrees of openness and structure, ranging from low degree of structuring to strong degree of structuring (Jacobsen, 2015):

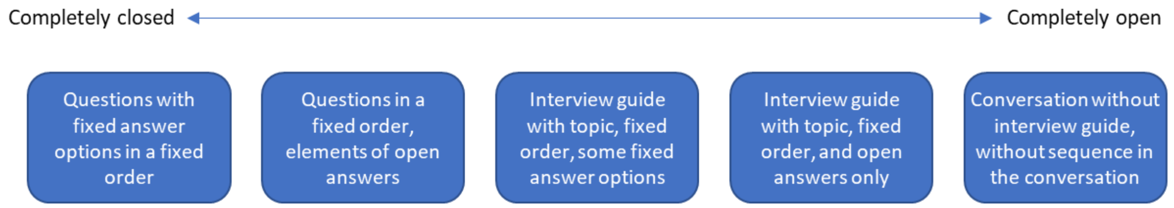
Completely closed
Completely open
Questions with fixed answer options in a fixed order
Questions in a fixed order, elements of open answers
Interview guide with topic, fixed order, some fixed answer options
Interview guide with topic, fixed order, and open answers only
Conversation without interview guide, without sequence in the conversation

Figure 5; Different degrees of interview structuring according to Jacobsen (2015)

In the middle of figure 3 is the semi-structured interview, which will be the approach used in this thesis. The benefit of a semi-structured interview is that it has an interview guide that includes a list of topics to cover during the interview. This ensures that important and relevant topics are discussed, and that information and data needed to answer the research questions is gathered.

Due to the ongoing pandemic (Covid-19), and geographical distances to some of the interview participants, the interviews will be conducted using Teams, Skype, or other suitable video conference solutions. The purpose of the interview will be communicated, both in the interview guide and before conducting the interview, and the participants will be informed that the interviews will be recorded – they will also be informed that the recording will be deleted as soon as the transcription process is finished.

3.3.3 How data was collected

Prior to writing this thesis, the knowledge about how the procurement process worked at Norwegian hospitals were limited. Therefore, some conversations were had with representatives from Sykehusinnkjøp to understand their involvement, and what kind of role they played in aiding the hospitals and health regions in procurements.

Based on this knowledge, four different health regions were contacted, in addition to two privately owned hospitals. Out of these six, only two answered initially. In the first interview, the participant shared names on two other stakeholders that should be contacted to provide a solid data foundation. Therefore, three persons, working on different levels from highly strategic to more operational, were interviewed from one of the health regions. Simultaneously, continuous attempts were made to get feedback from the three other health regions, which finally resulted in two of them participating in the study.

At the same time, the two private hospitals were also contacted, but only one of them agreed to participate in the study, while the last hospital declined, since they did not want to share details regarding their procurement process.

Interview documentation

All interviews except one were conducted using Teams, the last being conducted in person. The interviews that were conducted via Teams were recorded, and the recording stored on NTNU’s OneDrive for later transcription. The physical interview was conducted in a meeting room, where notes were taken during the interview.

3.3.4 Interview guide

To structure the interview, an interview guide should be used, especially in qualitative studies to ensure that all facets that should be discussed gets discussed (Jacobsen, 2015). The interview guide in this thesis had a more structured approach, where the interview questions was fully written out as opposed to being in the form of key words. Follow-up questions was asked when interesting and relevant subjects appeared.

The interview guide was sent to all participants in the study and contained information regarding where the study was conducted (institution and institute), which year, and the problem statement. Then, information regarding the length of the interview and how the interview was going to be conducted was included, in addition to information that the study would be anonymized to prevent potential vulnerabilities to be exposed to threat actors.

Finally, the seven interview questions was listed.

Interview questions

During the interviews, the following questions was asked:

1. Describe your role in the procurement process
2. How is cybersecurity considered in the procurement phase of digital medical equipment?
3. Are there any frameworks or best practices that are followed during the procurement phase of digital medical equipment?
4. Which stakeholders are usually involved in the procurement phase of digital medical equipment?
5. Does any of these stakeholders have cybersecurity competence?

6. Based on your experience, what do you think could and/or should be done to improve cybersecurity in the procurement process?
7. How do you safeguard/ensure that the cybersecurity considerations in the procurement process is followed?

In some of the interviews, follow-up questions were asked to dig deeper into the different subjects that were discussed. These were highly situational.

3.4 Selection of units

A challenge with doing research and surveys, is that we rarely can examine everything and everyone we want. This is particularly true for qualitative research, due to the time that needs to be put into individual interviews. Therefore, a selection of units must be done – this is referred to as a section, and can involve themes and phenomena's, context and time, people, and events. To safeguard the credibility of the thesis, a careful selection of units has been done. The focus will be on selecting the right theme, context and time, people, and events (Jacobsen, 2015).

The problem statement has three underlying research questions:

1. Which cybersecurity considerations is recommended to be taken in the procurement process of digital equipment, according to well-known frameworks and best practices?
2. Which cybersecurity considerations are taken at Norwegian hospitals in the procurement process of digital medical equipment today?
3. How could the current procurement practice of digital medical equipment at Norwegian hospitals be improved when it comes to cybersecurity?

The theme for these questions is cybersecurity considerations, the context is Norwegian hospitals and health institutions, the time is around the first quarter of 2022, and the event is the procurement process of digital medical equipment.

To gather information that can provide answers to research question 2 and 3, information must be collected from those responsible of procuring digital medical equipment in different Norwegian hospitals by interviewing them on which cybersecurity considerations they take in the procurement process of digital medical equipment.

Some institution might have outsourced some or all their IT services to partners or external vendors, and in those cases, there might be a need to interview those partners if they are involved in the procurement process.

To answer research question 1, a literature study will be performed, identifying recommendations, standards, frameworks, and best practices from national organizations, as well as well-known and well-reputed organizations. One of the criteria for independent organizations, is that they offer a certification that can be obtained through an audit performed by a third party.

As mentioned in chapter 2.4, the organization of Norwegian hospitals is divided into four regions North, West, Mid, and South-East. Together, these four regions own 25% each of a common procurement organization called Sykehusinnkjøp. This organization is tasked with carrying out procurement on behalf of the four regions and their hospitals. With that in mind, Sykehusinnkjøp will be interviewed to investigate the range of their responsibility, and whether they are involved in all sorts of procurement of digital medical equipment. By interviewing Sykehusinnkjøp, information needed to answer research question 2 and 3 will be gathered. Thereafter, the four regions will be contacted so that one hospital from each of these regions can be interviewed to gather further information that can contribute to answering research question 2 and 3. Additionally, hospitals outside this arrangement will be contacted, to investigate any differences that might be present.

Together, the breadth of this information will provide the foundation to answer the research questions and problem statement, hence creating a foundation of knowledge to say something general about which cybersecurity considerations Norwegian hospitals take in the procurement process of digital medical equipment today.

3.4.1 Selection criteria for informants

Taking a top-down approach, Sykehusinnkjøp is a natural entity to reach out to and interview due to their involvement and responsibility. The assumption is that Sykehusinnkjøp has an overarching procurement process that is followed by the different health regions, and consequently by the hospitals within those regions.

Then, there are the four different health regions. To limit the time spent gathering information by conducting interviews, one hospital from each of these health regions will be contacted. Larger hospitals have greater activity – they offer a wider range of services, and therefore need a larger amount of digital medical equipment. This entails that they are more frequently involved in the procurement process, which likely makes them more aware of the considerations that must be taken in the procurement process. The assumption is that they are more likely to have a more nuanced view and a deeper understanding of the elements and importance of the procurement process. Therefore, the largest hospitals will be the primary goal to interview.

To broaden the data base, the goal is to interview two hospitals outside the procurement process of Sykehusinnkjøp. The purpose of this is to shed light on potential differences in considerations that are taken in the respective procurement processes, and possibly contribute to sharing important considerations and best practices that are not currently taken into account. The only selection criteria for these hospitals, is that they are private hospitals, in addition to being over 1000 employees.

Finally, there is the selection criteria for the informants themselves. As mentioned in the beginning of this chapter, it is important to get as close as possible to those responsible for the procurement process so that the most correct and relevant information is gathered before answering the research questions. The selection criteria's is therefore that the informant is part of the procurement process today, and that the informant preferably have some extended experience with the procurement process.

The setup can be visualized in the following way:

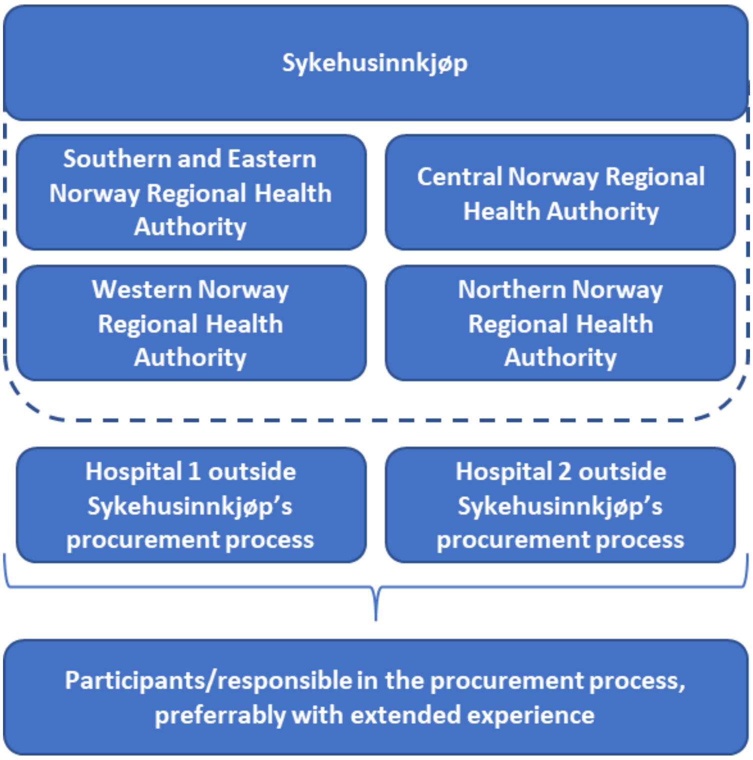
Sykehusinnkjøp
Southern and Eastern Norway Regional Health Authority
Central Norway Regional Health Authority
Western Norway Regional Health Authority
Northern Norway Regional Health Authority
Hospital 1 outside Sykehusinnkjøp's procurement process
Hospital 2 outside Sykehusinnkjøp's procurement process
Participants/responsible in the procurement process, preferrably with extended experience

Figure 6; Top-down approach of selection of units

3.4.2 Selection criteria for frameworks and best practices

The following selection criteria has been chosen to ensure the quality of the information used to answer research question 1:

- The framework or best practice is part of a public and well-known auditing process.
- The framework or best practice is published by a governmental body.
- The framework or best practice is published by an organization with a particularly good reputation, that references their work to leading information and cybersecurity related standards.
- The framework or best practice contains security controls and considerations that are specific to the procurement process.

3.4.3 Selection of informants

In addition to interviewing Sykehusinnkjøp on their role and responsibility in the procurement process of digital medical equipment, each of the different health regions will be contacted through their official contact email, using a generically crafted email. This email will contain information regarding the master project, the purpose of the interview, and information about how the interview will be conducted, how data will be collected, stored, processed, and deleted. The email will also ask for a contact person that is involved in the procurement process of medical equipment. The email that was sent is attached at the end of this thesis.

3.4.4 Selection of frameworks and best practices

There are several frameworks and best practices that adheres to the selection criteria. These frameworks and best practices contain security controls and considerations designed specifically with the procurement process in mind:

- NIST Special Publication 800-53 Revision 5
- COBIT 2019
- Center for Information Security (CIS) Controls
- Information Security Forum Standard of Good Practice
- Norwegian National Security Authority (NSM) Basic Principles for ICT Security

Therefore, to answer research question 1, this thesis will focus on which security controls and considerations that should be taken according to these frameworks.

3.4.5 About the participants

Six interviews were conducted for this master's thesis. The participants were chosen based on the health regions they were working in, to ensure that general information for the health region was gathered. All the participants had some sort of relation to the ICT department, and nearly all of them had cybersecurity expertise, with an overarching responsibility or knowledge of how information and cyber security is considered in their respective region.

Initially, the plan was to interview at least one representative from each health region, but that proved to be difficult – one of the health regions never responded, even after several requests. However, two of the informants mentioned that the framework they used was derived from a joint effort between them, which means that three health regions take some of the same considerations and have some of the same requirements in the procurement process.

Three representatives from Northern Health Region were interviewed, one from the Western Health Region, one from the Southern and Eastern health region, and one participant from a private hospital. The answers are, however, very similar across the different health regions and hospitals.

3.4.6 How the participants in the study was contacted

All participants in the study were contacted by email. These emails were sent to public email addresses, located on the homepage of the respective hospitals or health regions.

Initially, Sykehusinnkjøp was contacted to determine their role and involvement, before inviting representatives from the health regions and the hospitals themselves. According to Sykehusinnkjøp, they were involved in larger procurement processes, but as mentioned in the theory chapter, they needed support from the different health regions in terms of information security competence in the procurement process.

After understanding the role that Sykehusinnkjøp have, invitations were sent out to hospitals from all the four different health regions. Additionally, some of the participants provided names on people, which then were contacted directly.

3.5 Data analysis

The interviews and literature study will result in a large amount of information and data that needs to be analyzed. One of the first things that needs to be done, is to reduce the complexity by simplifying and structuring the information. The desired result of the data analysis is to add knowledge regarding a subject, and to be able to do this, the interviews, observations, and documents must be structured and compiled to point out connections, patterns, regularities, deviations, and possible causal relationships.

Practical analysis of qualitative data will revolve around four conditions (Jacobsen, 2015):

a) Documentation – the main task in this phase of the data analysis will be to describe the material that is gathered through interviews and literature study and explain the value and context they provide to answer the research questions and problem statement.
b) Exploration – thereafter, a review of the contents of the documentation will be performed, to explore and identify observations and findings that "stands out".
c) Systematization and categorization – in this phase, the documentation will be systematized and categorized so that they can be used to answer the different research questions.
d) Connect – in this phase of the data analysis, relationships between different categories will be drawn to see if there are any interesting connections.

To be able to thoroughly answer research question 2 and 3, interview questions must be constructed in such a way that they provide adequate amounts of information. The goal is to construct questions that reduce the potential need to review and improve the interview questions and redo interviews to obtain information that is necessary to provide quality answers to the research questions.

For research question 1, standards, frameworks, recommendations, and best practices will be examined to identify what the common security controls and/or recommendations are for the procurement process of digital equipment. Then, those controls will be summarized.

3.6 Reliability and credibility

Reliability and credibility refer to the trustworthiness of the data, and consequently, the conclusion. An example of reliable data is when a phenomenon is observed, and the result is fairly similar each time (Jacobsen, 2015).

To be able to answer the research questions and the problem statement, the collected data must come from sources that provide answers that reflect reality. What this entails, is that the correct people are interviewed to provide answers, in other words, those responsible for the procurement process at the different hospitals. To ensure that the right people are interviewed, and thus safeguard the reliability of the collected data, a thorough explanation of the purpose of the thesis must be sent, and what the objective of the thesis is. This will prevent the wrong people from being involved, and thus reduce the risk of unreliable data to be collected, in addition to wasting time.

3.6.1 Validity

While reliability refers to the trustworthiness of the data, validity refers to the relevance of the data that is collected. The collected data might be reliable, but also not so selective that it does not show the complete picture (Jacobsen, 2015). An example is asking cybersecurity expertise at a hospital about cybersecurity considerations during procurement – if it is not clear that we are seeking how it is done in daily operations, they might provide answers on how they would like to do it. These answers might be correct, but they would not answer the problem statement.

Validity is divided into two categories: internal and external validity. Internal validity refers to whether the data we have collected can be used to substantiate our conclusion, hence it is important to ask the right question during the interviews to gather sufficient quality data. External validity refers to whether our findings are transferrable to other, similar situations – i.e., would the result be the same if we asked another set of hospitals?

3.6.2 Strengths and weaknesses of the collected and utilized data

When collecting data about a phenomenon, it is important to talk to the right resources. In this thesis, information has been requested specifically from those involved in the procurement process, to ensure that the collected data reflects reality. The interviews were conducted over a three-week period in March and April of 2022, which means that the possibility of any major changes to how equipment is procured will be unlikely. The first interview question (describe your role in the procurement process) is included to ensure that a primary source of information is participating in the study. Primary sources are sources that are as close as possible to the phenomenon we want to observe (Jacobsen, 2015), which means that there is a high probability that the quality of the answer is as good as it gets. All the participants informed that they were directly involved either in the procurement process, or that they were closely involved. One of the participants informed that some of the questions had been discussed internally before the interview, to provide information that was as accurate as possible. Therefore, the strength of the collected data is estimated to be high.

A possible weakness of the collected data in the interviews, is that the participants not necessarily tell the entire truth about the procurement process or provide information that is different from reality to appear more mature. This difference between what you are saying, and what you are doing (theory and practice) is something to look out for, but no such signs were picked up on during the interviews – the participants seemed to show great levels of integrity in their answers.

3.6.3 Potential impact and consequences on the research and conclusion

The collected data is perceived to be reflecting the reality as it is. Credible sources were used throughout the data collection; hence the data seem to be trustworthy. The data is also valid for answering the problem statement and research questions; hence the data can be deemed as relevant. Additionally, it is also worth mentioning that the thesis seems to have a high degree of transferability, due to a lot of the information being collected from participants that are responsible for the ICT in their region, which entails that the hospitals in that region are following the same procurement process.

3.7 Ethical considerations in the survey

As with all research, there are important ethical guidelines which will be described in this section. Ethical dilemmas might occur in several circumstances during a research process. One crucial aspect is to have the right balance between which research results are presented and what potential consequences it may have for the participants or others who may be affected by the study (Jacobsen, 2015). With cybersecurity being so important, especially for hospitals caring for those in need, it is paramount that results does not reveal vulnerabilities that might be exploited by cybercriminals, which might cause severe consequences.

3.7.1 Informed consent

Everyone participating in this study have received an invite to participate in the study, with information regarding the purpose and theme of the study. Only those that voluntarily accept the invitation will be considered participating informants in this study (Jacobsen, 2015).

Jacobsen points out four important considerations that should be taken (Jacobsen, 2015):

- The right competence – the invitation to potential participants will include an interview guide that clearly states what the purpose of the interview is, and what the expectations to the interview are. By doing that, the risk of involving persons that does not have the right competence to answer my interview questions are minimized.
- Voluntary participation – the invitations that are sent will clearly state that the participation in the study is totally voluntary. That means that those uncomfortable with being interviewed can decline the invitation.
- Full information – as mentioned, an interview guide explaining the purpose, scope, goal, expectations, and so on, will be sent to the potential participants prior to the interviews. This interview guide will clearly state how data will be processed, used, gathered, stored, and deleted. Additionally, it will point out eventual advantages and disadvantages of participating in the study.
- Understanding – it is important that the participants also *understand* the information they receive. Therefore, clear language, structure, and easy to understand wording and sentences will be prioritized when inviting participants.

3.7.2 Receiving participants' consent

To get the participants consent, a request for a contact person was sent to the different hospitals. Thereafter, more in-depth information was provided to potential participants. This information was based on the template from the Norwegian Centre for Research Data (NSD, 2022), which included information about which interview questions that were going to be asked, the estimated length of the interview, how data would be recorded, processed, stored, and eventually deleted. The email to the participants also included a request for a date and time for conducting the interview, and information that accepting the invitation was considered consent to participate. Additionally, the participants were informed that they had the possibility to withdraw their consent at any time, either before, during or after the participation.

3.7.3 Right to privacy

Just as important as getting consent, is the participants right to privacy (Jacobsen, 2015). There are three elements that should be considered when it comes to privacy:

1. How sensitive is the information that is gathered?
2. How private is the information that is gathered?
3. What are the possibilities of identifying individuals base on the information that is gathered?

When it comes to question 1, the information that is gathered might very well be sensitive, and in that regard, all participants are being anonymized to prevent potential vulnerabilities being exploited through this thesis.

Regarding question 2, no private information is gathered, other than the role the participants have in the procurement process. This is only to understand the role of the participant and to safeguard that the correct persons involved in the procurement process are being interviewed.

The possibility of identifying individuals based on the gathered information is estimated to be very low – neither title, gender, location, or age will be used in the thesis, and the selection we are working with are large enough to prevent direct identification.

Overall, the privacy of the participants is assessed to be good.

3.7.4 Consequences of participating in the study

There should be no negative consequences of participating in the study – as mentioned in the chapter above, several precautions are taken to safeguard the privacy and anonymity of the participants in the study.

There are three elements that could identify participants: email address (specifically the acceptance email to participate in the interview), sound and video recording. The sound and video recording will be deleted as soon as the transcription is done, and no later than the deadline for delivering this master thesis.

However, there are some potential positive consequences by participating in the study: without sharing specifics about which hospitals that use certain practices, all good and interesting practices have been shared with other participants in the study, sometimes as part of a follow-up questions or if someone has asked for advice. Additionally, all participants that have requested a copy of the thesis will receive a copy once the thesis has been submitted and given a grade, so that they can use the thesis and compare it to their current practice, and thus potentially improve their own procurement processes.

3.7.5 License and notification obligation

To be allowed to gather information through interviews, a request form for data collection has been submitted to the Norwegian Centre for Research Data (NSD) (Jacobsen, 2015). The request form contained several questions that needed to be answered, such as information regarding the project, selection of units, documentation, type of information, how to process collected data, information security, durability of the project, and so on. The request was approved by NSD in the end of February 2022.

3.7.6 Requirements for proper presentation of data

It is important that results from the interviews are presented correctly, and not taken out of context (Jacobsen, 2015). Citations should not be taken out of context to prove a point it is not supposed to prove, but only used to answer an interview question or to substantiate an observation in relation to an interview question. Even though it is important to acknowledge that answers cannot be presented in full, and that data analysis will lead to a reduction in details, it is equally important to strive for a complete reproduction of an ideal.

Another important point is to avoid cherry-picking answers to prove a point one thinks is important, or even worse, to alter answers to make them fit into a story we want to tell. As researchers, it is our obligation to reproduce explanations as they were told, so that the integrity of the research stays intact.

4 Results

In this chapter, the findings from the interviews will presented, in addition to a summary at the end of the chapter, highlighting the commonalities between the health regions.

4.1 Findings from the interviews

During the interviews I experienced that four of the interview questions were answered across each other, therefore, I merged four of the interview questions that were related. Thus, the questions are compiled into the following four interview questions:

1. Which cybersecurity considerations are made in the procurement process of digital medical equipment, and are there any frameworks or best practices that are followed or used to set requirements?
2. Which stakeholders are usually involved in the procurement process of digital medical equipment, and does these stakeholders have cybersecurity competence?
3. Based on your experience, what do you mean could and/or should be done to improve cybersecurity in the procurement process?
4. How do you safeguard that cybersecurity considerations and requirements are considered in the procurement process?

The results from the interviews will be presented underneath each question, consisting of statements from each of the interviewees.

Question 1: which cybersecurity considerations are made in the procurement process of digital medical equipment, and are there any frameworks or best practices that are followed or used to set requirements?

All the participants informed that it varied how much they were involved in the procurement phase, which directly impacts which considerations that are taken. However, the informants said that they had an overlaying information security management system (ISMS) that were based on ISO27001 or similar. Additionally, none of the equipment was implemented without considering cybersecurity, the challenge was usually to implement security measures to safeguard the information due to missing security functionality in the equipment. All the interviewees informed that they follow the Norm of information and cybersecurity, especially the guidelines for medical technical equipment.

Two of the regions additionally informed that equipment that was not considered under the IVDR underwent stricter requirements in the procurement process when it came to patching capabilities, identity and access management, password and authentication mechanisms, and similar.

Although not everyone had the same level of cybersecurity maturity, all the participants had some sort of work related to safeguarding cybersecurity in the procurement process, however, not everyone had been able to implement these controls and policies yet. Consequently, some procurement processes failed to involve the IT department with adequate cybersecurity competence early enough in the procurement process, resulting in the abovementioned workaround, which is to implement compensating measures to ensure secure operations.

One of the regions were in a pilot phase of implementing a procedure for procurement of imaging and radiation therapy equipment, which was their largest expense post within medical technical equipment. This procedure, called Strategy for Medical Technical Equipment, included a guideline for procurement, where, among others, Sykehusinnkjøp had contributed with experience and input. However, when asked, this procedure and guideline was meant for that specific region. An interesting detail from this procedure, was the appointment of an ICT cybersecurity coordinator role, that is meant to oversee the lifecycle management of hardware such as medical technical equipment.

One of the other regions already had this role (ICT cybersecurity coordinator) implemented, which had the overarching responsibility for lifecycle management of hardware devices. Due to the role being fairly new, the role was not fully involved in all procurement processes yet, but the holder of the role informed of an increased awareness and participation in procurement processes. Additionally, this region had prepared a range of documents with *mandatory* requirements and *recommended* requirements. These requirements were made in cooperation with representatives from two other health regions, which means that these other two health regions use the same type of requirements as well. The documents considered both privacy, information security, and operational security, in addition to a questionnaire for simple mapping of information security in medical technical equipment. The same informant mentioned that if the equipment had a CE-certification, they usually requested the vendor for information whether there were any cybersecurity deviations in the certification, since CE certification contains several cybersecurity requirements.

One health region stood out when it came to their level of maturity. This region had clear roles and responsibilities, dedicated medical technical personnel that was an integrated part of the lifecycle management of digital medical equipment, such as the procurement process, and they had regular meetings where equipment that needed to be procured was discussed also in terms of information and cyber security. The participant from this region informed that they used the same framework as the participant mentioned in the section above, which was a combination of joint effort and inherited documentation.

Almost every one of the participants in the study informed that they were conducting risk and vulnerability analyses (RVA), which included different cybersecurity considerations. Some of the participants informed that they only did RVA's on the larger vendors, while others did it after the procurement process, but before the implementation process. Some of the participants also performed RVA's later in the lifecycle, more information on that in the last section.

Multiple of the participants also mentioned that many vendors hold too much power, and often dictates what kind of cybersecurity measures they implement in their equipment. The challenge is that there are a limited number of vendors for certain types of equipment, so the hospitals are at the mercy of the vendors, and sometimes must adjust their information security management systems (and their requirements) to implement their equipment.

Two of the hospitals also mentioned that their data processor agreements set some requirements and guidelines for their procurement process, by referring to the Norm.

Question 2: Which stakeholders are usually involved in the procurement process of digital medical equipment, and does these stakeholders have cybersecurity competence?

Most of the interviewees mentioned the same challenges in being involved early enough in the procurement process. However, everyone experienced an involvement at some stage. The problem was that the later they got involved, the more compensating measures had to be taken.

Common for everyone was that the need arose in the clinic, with nurses, doctors, and similar needing new equipment, either due to the equipment needing replacement or to offer new or better treatment methods.

Thereafter, the medical technical department usually got involved. At this stage, the interviewees reported on different experiences, due to the range in cybersecurity competence in the staff working in the medical technical department.

For larger procurements, Sykehusinnkjøp was involved as well, although they (historically) did not necessarily have adequate information and cyber security expertise to fully consider whether the level of security was acceptable. Being aware of the need for information and cyber security expertise, Sykehusinnkjøp would therefore inform the ICT departments either locally or regionally to ensure that this competence was involved in the procurement process.

Finally, the ICT department was involved, and for all the interviewees, that meant that at this stage, information and cyber security expertise was involved.

Some of the participants reported on a slight shift towards the ICT department being involved earlier, due the experienced consequence in the clinic of prolonged projects when the ICT department was not involved. One of the interviewees particularly mentioned that the clinic had learned this "the hard way", and this awareness had resulted in earlier consultation.

As mentioned in question 1, the region that had appointed a dedicated role as ICT security coordinator for medical technical equipment reported that they experienced an increased involvement earlier in the procurement process, and the region that already has this role implemented for a while, experienced that they were involved in all relevant procurement and could evaluate the equipment in terms of information and cyber security.

Another common observation was that when the timeframe for procuring new equipment was short, or equipment needed to be procured urgently, the ICT department was usually not involved, however, planned projects usually meant greater involvement.

One of the regions also reported that they had established their own forum for regional procurements of medical technical equipment, where all the hospitals were represented.

Most of the interviewees underlined that they wanted to be involved earlier in the process, and that they worked towards that.

Question 3: Based on your experience, what do you mean could and/or should be done to improve cybersecurity in the procurement process?

There were many good suggestions on how to improve the cybersecurity considerations and requirements in the procurement process. The suggestions range from national level to individual level; hence they will be presented in a top-down approach.

Many of the interviewees informed that there is too much autonomy both in the clinics, in the hospitals, and in the regions. Therefore some, but not all, suggested a clearer national standard for the requirements. Two of the participants meant that this could have a positive impact on the vendors, since they would not need to adapt their equipment to comply with several different sets of requirements from different health regions and/or hospitals, but rather produce more standardized equipment that was compliant to a national standard. Another participant mentioned that some of the requirements in the Norm could be improved when it came to the procurement process, while another participant suggested dynamic procurement processes where vendors could get prequalified so that they did not have to reinvent the wheel every time they procured equipment. However, one participant mentioned that even though the hospitals are part of the public sector, they are organizations that have their own Chief Executive Officers, running daily operations just like a private company, with a range of different systems – therefore, the participant was not sure how easy it would be to introduce an overarching system that could be used by all hospitals, due to the huge complexity.

Without going into specifics, one participant mentioned the challenge of some legislations occasionally coming into conflict with each other, for instance some privacy and information security requirements.

As previously mentioned, most of the participants wanted the ICT department to be involved at an earlier stage, preferably as soon as the need for new equipment had been reported. Two of the regions mentioned the newly invented role of an ICT security coordinator for medical technical equipment as a contribution to safeguarding information and cyber security requirements in the procurement process. Additionally, several of the participants mentioned clearer role and responsibility descriptions, and an expressed desire for the medical technical department to take a greater part of the responsibility for information security in the lifecycle management (including procurement) of medical technical equipment. One participant mentioned that medical technical equipment usually had a lifespan of 10 years before vendors usually ended support and suggested that the medical technical department took responsibility for planning of exchanging old equipment that had gone out of vendor support. The same participants informed that some equipment in their region sometimes had to be procured urgently due to under-budgeting – the different hospitals in the region might need 10 units of something, but only getting the budget of one. Consequently, patients might need to be transferred to other hospitals, waiting lists would increase, and the total cost of this would surpass the cost of procuring the equipment in the first place.

Another thing that was mentioned, was the alternative way procurement was done in USA; there, vendors had to fill out a form (MDS-2) before the hospitals conducted a RVA on the result. However, the participant suggesting this did not think this would work as good in Norway, due to the hospitals being so much smaller than in the US.

In addition to clearer role and responsibility descriptions, some of the participants mentioned the need for creating good checklists that should be followed during procurement. This was already implemented by two of the participants in the study, however not fully in use yet in one region due to the clinic not being aware of it yet. The other region informed that due to their level of planning, these requirements were considered in most, if not all, procurements of digital medical equipment. The same participant mentioned that they also had meetings with Melanor, which is a Norwegian industry organization for competence companies that develop and supply medical equipment, laboratory equipment, measuring equipment and aids in the Norwegian market. They experienced a growing focus on information and cyber security from this organization, which is a good sign since one of the goals of Melanor is *to work actively to ensure that the industry complies with current ethical standards, the authorities' requirements for quality and security, and makes proposals where they see room for improvement* (Melanor, 2022).

Finally, many of the participants mentioned that the awareness and competence in the clinic should be raised. By having fundamental understanding of which information and cyber security considerations that should be taken in the procurement process, the clinic could very well contribute to raising the overall security of the equipment in the hospital.

Question 4: how do you safeguard that cybersecurity considerations and requirements are considered in the procurement process?

The participants had varying modus operandi when it came to auditing the cybersecurity considerations in the procurement process. Several mentioned that RVA's were conducted and updated after the procurement to ensure that the requirements were met, and that risks were properly mitigated. Some had solution architects that reviewed cyber security in the implementation phase and identified whether there were any discrepancies between what the vendors had promised and what had been delivered.

One participant mentioned that a contract review sometimes were conducted to assess whether there were any discrepancies as well.

Additionally, one of the participants said that "*if all medical equipment used in hospitals is to satisfy the legal requirements, it means the end of patient treatment*".

4.2 Summary of findings

Some themes repeated themselves during the interviews, and these have been summarized in this chapter:

- Most of the participants mentioned that they would want to be included earlier in the procurement process. An advantage of being involved from the start is that it enables you to ensure security *in the equipment itself*, rather than securing the environment the equipment will operate in after it is purchased. Well-planned procurements often included necessary cybersecurity expertise, however, equipment sometimes had to be procured urgently.

- All hospitals performed risk and vulnerability analyses of the equipment during the lifecycle of the equipment, however, early RVA's could prevent bad purchases and additional work of creating a secure operating environment in case the equipment does not have adequate built-in security. Some of the participants mentioned that even though RVA's very done, they sometimes were not followed up on afterwards.

- Many of the participants mentioned that clearer role and responsibility descriptions could also attribute to raising the cybersecurity maturity, by appointing clearly defined tasks to different stakeholders in the procurement process.

- Some of the participants meant that medical technical departments should be more involved by getting increased ownership in the procurement process, in addition to increased cybersecurity competence regarding medical technical equipment.

- Many of the participants mentioned a need for increased cybersecurity awareness and fundamental cybersecurity competence in the clinic.

- Many of the participants mentioned that it would have been an advantage if the equipment vendors had less control over which security measures their equipment had, and instead adapted to requirements of the hospitals, or alternatively, a national standard.

5 Discussion

The problem statement for this Master thesis is to investigate how aligned Norwegian hospitals are with well-known cybersecurity frameworks when it comes to cybersecurity considerations in the procurement process of digital medical equipment. The problem statement has three underlying research questions, which seeks to unveil which cybersecurity considerations that should be taken according to well-known frameworks, which cybersecurity considerations that are taken, and finally, if there are room for improvement in the current practice:

1. Which cybersecurity considerations is recommended to be taken in the procurement process of digital equipment, according to well-known frameworks and best practices?
2. Which cybersecurity considerations are taken at Norwegian hospitals in the procurement process of digital medical equipment today?
3. How could the current procurement practice of digital medical equipment at Norwegian hospitals be improved when it comes to cybersecurity?

In the subsequent subchapters, these research questions will be answered individually.

5.1 Which cybersecurity considerations are recommended to be taken in the procurement process of digital equipment, according to well-known frameworks and best practices?

According to well-known frameworks and best practices, there are several cybersecurity considerations that should be taken in the procurement process of digital equipment. Please refer to chapter 2.7 where frameworks and best practices are described in detail.

To summarize the controls from NIST 800-53, ISF Standard of Good Practice, and the Norwegian National Security Authority, the following model has been made (figure 7), showing a suggested workflow for procuring equipment. Please beware that the model simplifies certain aspects, such as the risk management process and pre-approving of the vendor, which is outside the scope of this thesis. Additionally, the risk and vulnerability assessment of the vendor may include other aspects to consider or requirements to meet, to determine whether the risk is accepted or not; this model has only taken commonalities from the frameworks and presented them. The model considers the different stakeholders in the procurement process, such as the clinic, the vendor, and the ICT department. The idea is that the ICT department can consult the medical technical department where needed, so that they are involved as well. If equipment is approved for procurement and then procured, it is important that the device is included into the device lifecycle management, where network traffic is monitored, the device is physically secured, and it is made sure that the equipment only can communicate with necessary systems only.

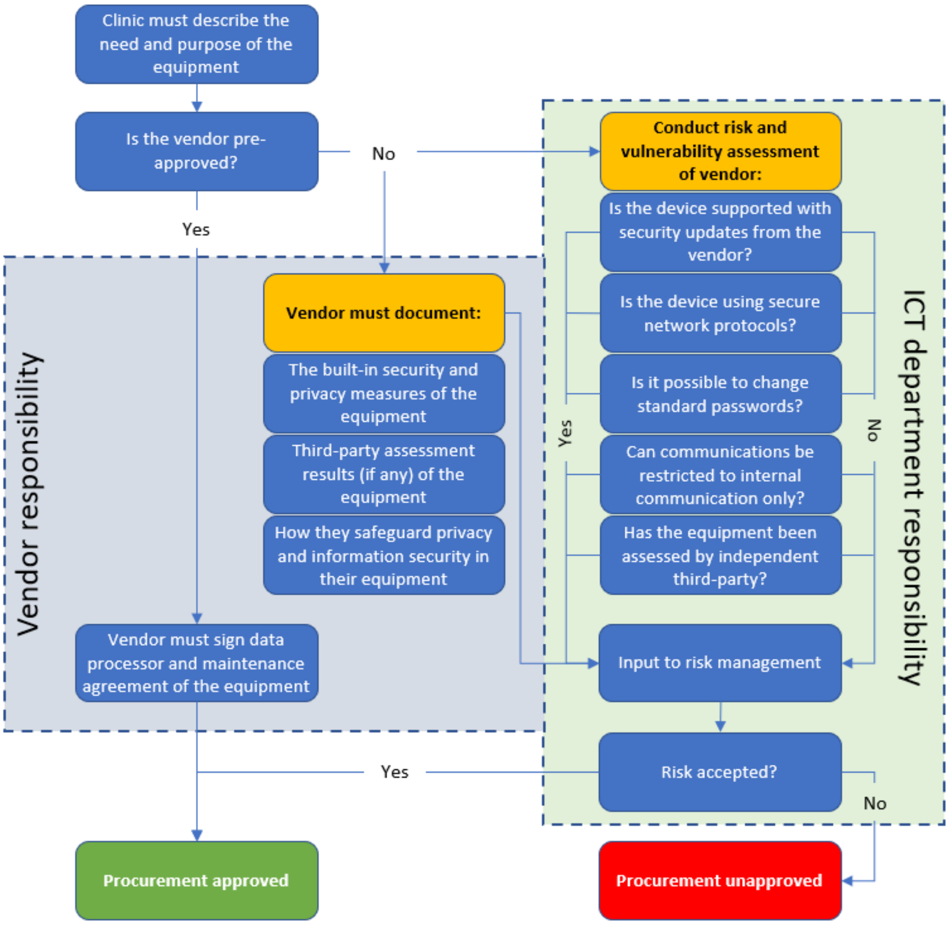
Clinic must describe the need and purpose of the equipment
Is the vendor pre-approved?
No
Yes
Vendor responsibility
Vendor must document:
The built-in security and privacy measures of the equipment
Third-party assessment results (if any) of the equipment
How they safeguard privacy and information security in their equipment
Vendor must sign data processor and maintenance agreement of the equipment
ICT department responsibility
Conduct risk and vulnerability assessment of vendor:
Is the device supported with security updates from the vendor?
Is the device using secure network protocols?
Is it possible to change standard passwords?
Can communications be restricted to internal communication only?
Has the equipment been assessed by independent third-party?
Yes
No
Input to risk management
Risk accepted?
Yes
No
Procurement approved
Procurement unapproved

Figure 7; Suggested model for workflow when procuring medical technical equipment

5.2 Which cybersecurity considerations are taken at Norwegian hospitals in the procurement process of digital medical equipment today?

Throughout the interviews, it was evident that the participants ranged from having highly mature procurement processes, to not being included until the equipment needed to be integrated in the network. Two of the participants shared their security requirements for when they procured medical technical equipment, which was derived from the health region that did not participate in this study. Hence, one could argue that three out of four health regions take almost the same cybersecurity considerations when procuring technical medical equipment. These two regions both had requirements that referred to compliance with the Norm (please refer to chapter 2.4.3 for relevant requirements from the Norm), in addition to other requirements such as identity and access management, authentication, secure networking, logging, and secure storage. The last region and the individual hospital were working to implement similar cybersecurity requirements; however, they were not fully operationalized yet.

The most mature health region (and consequently the hospitals in that region) appeared to take adequate cybersecurity considerations in the procurement process of technical medical equipment; they had a list of requirements divided into must and should, they had appointed dedicated roles, with defined responsibility, and they had involved themselves in the procurement process by participating together with the clinic. This is close to the recommended practice by Coronado and Wong, who states that the device lifecycle management starts in the procurement process (Coronado and Wong, 2014), and Schwartz et al. that recommend that IT departments are involved in the procurement process, and that clear requirements and risk assessments are prepared in advance (Schwartz et al., 2018). Additionally, this region participated in meetings with an industry organization to discuss cybersecurity in medical equipment, which is an important first step towards creating a common baseline, recommended by Schwartz et al.

One of the other health regions were not as mature yet but had similar requirements in place. However, they lacked the necessary personnel and routines to safeguard that the requirements were followed, although a dedicated role had been appointed and experienced a growing involvement in the procurement process.

The last health region was working on a strategy for procuring technical medical equipment, where a dedicated role for safeguarding cybersecurity in the procurement process was intended. However, due to this role not being ready, in addition to inadequate supporting routines for procurement, they experienced that they sometimes were left out of the process until the equipment was to be implemented into the infrastructure. Hence, few cybersecurity considerations were taken in the procurement process itself, which resulted in that compensating measures to be taken. The story was similar for the private hospital, however, the work of implementing a procurement procedure was ongoing.

Summarized, the findings are similar to what prior research have identified:

- All the participants had a list of considerations and requirements; however, they were not always included in the procurement process. Ensuring involvement of the IT department in the procurement process is an important step towards higher cybersecurity maturity, since it enhances the likelihood of cybersecurity

being considered both in the form of requirements and risk assessments. Only one participant appeared to be aligned with recommended practices from prior research.
- Limited cybersecurity awareness in the clinic is a challenge that can lead to IT departments being left out of the procurement process, increasing the possibility of insecure devices being procured
- Inadequate or absent procurement processes can lead to insecure devices being procured

5.3 How could the current procurement practice of digital medical equipment at Norwegian hospitals be improved when it comes to cybersecurity?

All the participants agreed when asked if there could be done anything to improve cybersecurity in the procurement process. These improvement suggestions are described in chapter 6.2.

However, comparing recommended security considerations to which cybersecurity considerations that are *actually* taken, is equally valuable. Evaluating the delta between them enables us to determine what should be done to improve, given the fact that the recommended security considerations are part of well-known frameworks from industry leading actors. The comparison of the answers to research question 1 and research question 2 shows that there is room for improvement, generally speaking. Even though some of the regions have higher maturity than others, all the participants in the study agreed that there always was room for improvement. Looking at the suggested model in chapter 5.1 (figure 7, the most mature region is quite close to that model, which also shares similarities with the procurement process described by ENISA in chapter 2.8 (ENISA, 2020). It was outside the scope of this thesis (and the interview questions) to identify whether there was some sort of pre-approval of vendors, but other than that, the most mature region made sure to take responsibility to safeguard cybersecurity in their region.

Throughout the thesis, and especially the interviews, it has been observed that the challenge is not necessarily about the considerations that are taken at the hospitals in the procurement process, or whether the hospitals adhere to well-known frameworks and best practices, but rather that it seems that the hospitals are not properly set up for success. There seems to be several reasons for this:

- The different hospitals and regions seem to be very autonomous – projects are dependent on their participants to succeed, and results are not necessarily repeatable for similar projects, i.e., the same input might yield a different output. This is also evident in the reports from the Office of the Auditor General, and in the report from Lysneutvalget and its follow-up report St. Meld. 38 (see chapter 2.5), which states that neither the hospitals or health regions sufficiently cooperate or share knowledge between each other. It was evident in the interviews that the participants ranged from highly mature when it comes to safeguarding that cybersecurity considerations are taken in the procurement process, to the other end of the scale, where some of the participants experienced that they had to "put out fires".

- There exist ambiguities about who holds roles and what responsibilities these roles have – having a policy or a set of requirements is necessary, but if no one is safeguarding that the policies are followed, and requirements met, it will eventually lead to mistakes being made in the procurement process, which might lead to the introduction of insecure and vulnerable equipment into the infrastructure.
- Vendors have too much power in the delivery of medical technical equipment – several of the participants in the study reported that they sometimes had to adjust their requirements so that vendors could deliver necessary equipment. This also corresponds with findings from the Office of the Auditor General, which stated that the suppliers largely set the terms in the agreements. However, one of the participants did mention that they participated in regular meetings with the Norwegian industry organization Melanor, which worked towards medical equipment being up to Norwegian laws, regulations, and standards. The participant mentioned that Melanor, and its members, was interested in addressing information and cyber security concerns and to raise the baseline of cybersecurity. This is also a recommendation from the research paper cited in chapter 4.8, stating that hospitals should work together to show vendors that they take security seriously (Rios, 2015). Establishing a cross-regional forum, where participants from the health regions cooperate with vendors, could contribute to raise the overall level of cybersecurity in medical technical equipment.

Common for the recommendations from Lysneutvalget and the reports from the Office of the Auditor General is more governmental cybersecurity governance. Lysneutvalget (2015) specifically recommended "*stronger cybersecurity governance from the Ministry of Health and Care Services"*, elaborating that there is "*a need for stronger national management to identify and strengthen common needs and to avoid divergent solutions in the regions*". As mentioned in chapter 2.5, the OAG also recommends further involvement by the Ministry of Health and Care Services, by ensuring that the health regions and hospitals comply with current laws and regulations for information security and privacy, that the health regions ensure better coordination between regions and between hospitals internally in their region, that requirements for information security in medical technical equipment becomes more uniform, and that laws and regulations are followed by setting clear vendor requirements in the agreements. It seems that in the absence of adequate involvement, investment, and clear guidelines on way of work from the government, the health regions and hospitals are somewhat left alone to figure out how they want to operate. Consequently, the maturity level differs quite much, where some of the health regions have high focus on cybersecurity, which means that the respective hospitals in their region are well taken care of when it comes to information and cyber security, while other health regions experience an uphill battle to implement cybersecurity measures that safeguard the systems and infrastructure in their hospitals.

The more complex systems are, the harder they are to operate, manage, and secure. This does not only apply to technical systems, but also to people (implied: roles and responsibilities) and processes (way of work). A way of reducing complexity is through standardization, which can contribute to making systems easier to operate, manage, and secure. Standardization, however, is a strategic initiative that should be implemented from the top to ensure that all stakeholders have been involved and their concerns and needs have been addressed, which is paramount when it comes to the vital work of hospitals. With reference to the report from Lysneutvalget, it seems that there still is room for improvement when it comes to "*stronger national management to identify and strengthen common needs and to avoid divergent solutions in the regions*".

In the summary of the findings from the interviews, larger involvement of the ICT departments in the procurement process, and increased cybersecurity competence in the clinic, were elements that was mentioned by several of the participants. Doctors and nurses' main objective are to treat patients in an effective way so that they can be discharged, however, they also play an important role in the procurement value chain, like choosing which equipment they are going to use. The region with the most mature operating model had made sure that they were involved in the procurement process by planning procurement in advance together with the clinic. By doing this, they do not only safeguard that the equipment they procure have adequate security, but they also put themselves in a position where the cooperation between the ICT department and clinic can contribute to raising the cybersecurity awareness and competence in the clinic by addressing and discussing cybersecurity concerns in new systems and technology. Instead of just imposing a set of rules and policies on the clinic, they make sure to involve themselves, and hence set themselves up for success. Prerequisites for being able to do this are defined processes, requirements, and clear roles and responsibilities.

Norwegian hospitals are required to adhere to the Norm when acquiring medical technical equipment. However, the Norm is only a set of requirements, it does not provide a suggested or standard operating procedure. A suggestion is that instead of continuously reinventing the wheel across the different health regions, the government should create a somewhat flexible standard operating procedure, that considers roles, responsibilities, tasks, and suggested workflow. When they create this standard operating procedure, important stakeholders such as representatives from clinics, ICT and MTU departments, and vendor organizations, such as Melanor, should be included to make sure that all important considerations are made. This could contribute to safeguard that the considerations are taken, and requirements are met before equipment is procured.

The economic consequences of implementing such a standardized model have not been investigated, nor is it part of the scope of this master thesis. There are, however, some factors that point to lower cost over time when introducing standardization:

- **Reduced complexity** – standardization reduces complexity, which can lead to:
- **Increased effectiveness** – standardization can contribute to increased effectiveness, since defined processes makes work predictable; people know their roles and their responsibilities in that role. Standardization can also lead to:
- **Increased security and resilience** – standardization also contributes to increased security since it can reduce the amount of different technology in the infrastructure. Consequently, the environments will be easier to maintain, monitor, and manage. It might also require fewer people to operate, and be more resilient to cyberattacks.

Challenges with introducing a standardized model is the different amount of risk appetite across the different health regions and hospitals, however, this is something that might be good to discuss across regions as well.

5.4 Summary of discussion

Recommended security considerations

According to Schwartz et al. (2018) and Coronado and Wong (2014), it is recommended that a procurement process is created, that cybersecurity is integrated in the procurement process of digital medical equipment, and that cybersecurity expertise from the ICT department are involved in the procurement of said equipment. Figure 7 in chapter 5.1 shows a suggested model that adheres to security considerations from well-known frameworks and best practices. This model is not considered exhaustive in the sense that other requirements can be included, however, it considers the commonalities from NIST 800-53, ISF Standard of Good Practice, and NSM Basic Principles for ICT Security. The full list of considerations can be found in chapter 2.7.

Current state of art at Norwegian hospitals

The interviews revealed that the health regions are working very autonomously. Consequently, they are ranging from being close to what is considered the recommended way of working, while others are working to get there. The question is whether it is best to leave it to the health regions to figure out a way of procuring adequately secure digital medical equipment, or if it is better to create a national guideline that can contribute to this. During the interviews there was only one participant that mentioned a national guideline, and due to it being slightly outside the scope of the thesis, it was not a part of the interview questions. A recommendation for further research is therefore that it should be investigated whether a national, standardized procurement process could be implemented or not (see chapter 6.3).

The health region that is considered most mature when it comes to cybersecurity, had made sure not only to create a set of requirements and recommendations for the procurement process, but they also took an active role in the process, helping the clinic to plan procurements in advance. By doing that, they minimized the risk of being excluded in the procurement process, and effectively mitigated the risk of insecure equipment being procured, by compensating for the limited cybersecurity awareness in the clinic, as referred to both by Schwartz et al. (2018) and the other participants in this study. This health region was the only one in this study with this operating model which is very close to the operating model suggested in figure 7 in chapter 5.1, which is based on well-known frameworks and best practices such as NIST 800-53, ISF Standard of Good Practice, and NSA Basic Principles for ICT Security, described in this thesis. The challenge of reaching this level of maturity is believed to be inadequate time and personnel.

The other participants in the study informed that they were working on implementing similar models in their regions, however, the implementation timeframe is believed to be relatively different due to how far in the process they informed that they had come. Consequently, their resilience towards cybercriminals is believed to be reduced compared to the health region that had the model in place. Both Coronado and Wong (2014) and Schwartz et al. (2018) points out that inadequate security can lead to disruption of operation of medical devices and the availability and integrity of information on these devices, which in turn pose a threat to patient safety.

How the current procurement process could be improved

Looking at the answers from research question 1 and 2, it is evident that there is room for improvement in general. The system today is complex and, consequently, difficult to manage and secure. Both Lysneutvalget (2015) and The Office of the Auditor General (Riksrevisjonen, 2015) recommends a stronger cybersecurity governance from the Ministry of Health and Care Services, where Lysneutvalget specifically calls out for *"stronger national management to identify and strengthen needs and to avoid divergent solutions in the regions"*. As mentioned above, the current state of art is rather on the opposite end of the scale, with health regions working autonomously trying to figure out how to best conduct procurement. In their report, The Office of the Auditor General recommends further involvement from the health department to ensure compliance with laws and regulations across health regions, and that clear vendor requirements are set in the agreement. Additionally, they call for a greater cooperation across the health regions to ensure better coordination, and that requirements for information security in medical technical equipment becomes more uniform. This aligns with the study by Rios (2015) titled *Medical Devices have "A Long Way to Go"*, where the authors recommended more cooperation between hospitals to work together to raise the overall level of cybersecurity in digital medical equipment. The challenge appears to be twofold:

1. There is no suggested or recommended procurement process that is created on a national level, which leaves the hospitals to figure out the process for themselves, and
2. There seems to be inadequate cooperation with vendors to improve the baseline for built-in cybersecurity in digital medical equipment.

The consequence of the first challenge is that the wheel often must be reinvented across the different health regions, which can lead to unnecessary time consumption trying to identify a working operating model for procurement. Reinventing the wheel is also unnecessary if the operational model is repeatable, which seems plausible since it is a matter of patient treatment governed by the Ministry of Health and Care Services. Designing a standardized model in cooperation with stakeholders from the health regions, clinics, ICT and MTU departments could contribute to solve this challenge.

When it comes to the second challenge, only one of the regions mentioned that they had such cooperation today. In their experience, Melanor showed interest in contributing to raising the level of cybersecurity in digital medical equipment and adhering to relevant laws and regulations. The discussions in this forum could contribute to raising the level of cybersecurity in digital medical equipment in other regions as well, given that the forum consists of the same vendors.

Introducing a standardized model for procurement will contribute to decrease the complexity, consequently increasing the level of cybersecurity in the hospitals and their resilience towards cybercriminals and cyberattacks. Increased cooperation with vendors can contribute to raising the level of cybersecurity in the digital medical equipment itself, which also contributes to making the hospitals more secure.

5.5 Limitations

Although participants from three out of four health regions participated in the study, there might still be ways of working in other hospitals that are different from the findings from this study. The participants mainly consisted of representatives from the ICT department or similar, which could skew the results towards their experience – none of the participants in the study were stakeholders from the clinic or the medical technical department, who might have had other experiences when it comes to the procurement process.

There is also worth mentioning that the results in this thesis is made up of information that is being conveyed, and not experienced in person. However, the participants appeared to show great integrity in their answers, making it more than likely that the reality is described.

6 Conclusion

This thesis set out to seek an answer to which cybersecurity considerations that were taken in the procurement process of digital medical equipment at Norwegian hospitals today. The problem statement has three underlying research questions, which seeks to identify which cybersecurity considerations that should be taken in the procurement process according to well-known frameworks, which cybersecurity considerations that are taken in the procurement process at Norwegian hospitals today, and finally, how the procurement process at Norwegian hospitals can be improved when it comes to cybersecurity considerations.

Looking at the answers from the participants in the interviews, it is evident that although an improvement has been made in terms of cybersecurity posture since the report from Lysneutvalget in 2015 and the OAG report in 2016, some of the findings in those reports are still existent to this day. Especially the report from Lysneutvalget called for *stronger national management to identify and strengthen common needs and to avoid divergent solutions in the regions*. However, there is still very limited standardization across the different health regions, who works very autonomous and independent to each other. Consequently, the maturity when it comes to cybersecurity considerations in the procurement process is vastly different from region to region, leaving some regions to be more prone to cyberattacks. Additionally, the apparent lack of national management to endorse standardization, not only when it comes to technology, but to people and processes as well, means that the maturity gap will take unnecessary long time to close.

As mentioned throughout this thesis, the procurement process sets some precedents for the possibilities to secure the device later in its lifecycle, such as the ability to change standard passwords, install security updates, and define access through identity and access management. Therefore, the focus should be on ensuring that the right cybersecurity considerations are made in the procurement process, and that vendors delivers according to requirements, so that critical infrastructure vital to patient treatment can be properly safeguarded. Until a more standardized way of work has been developed, the complexity within the health regions and the differences between them, will continue to grow.

Not only should the right considerations and requirements be prepared, but they should also be an integral part of the procurement process as soon as the need for equipment has been described. Several of the participants in the study mentioned that they were not involved until after the equipment had been procured, which meant that compensatory measures had to be introduced. This is a consequence of the lack of maturity and is something that could have been solved by preparing a standard procurement process, where the ICT department was involved. A suggestion is shown in figure 5 in chapter 5.1.

Therefore, the conclusion of this thesis is that Norwegian hospitals to some degree are aligned with well-known frameworks and best-practices when it comes to which cybersecurity considerations that should be taken in the procurement process of digital medical equipment. However, the considerations and requirements they have prepared are not necessarily taken into account in the procurement process, due to missing involvement of cybersecurity expertise in the procurement process. Consequently, equipment with inadequate security is sometimes procured, which means that compensating measures must be put in place to safeguard the cybersecurity and privacy in the rest of the infrastructure.

6.1 Recommendations to the health sector

The health sector today is implementing several measures in the right direction to improve cybersecurity in hospitals and health care institutions. There are nonetheless room for improvement. Taking the following actions could contribute to elevating the cybersecurity in the procurement process:

- Get management support to ensure that all digital medical equipment follows a defined procurement process, where the IT department is involved from the planning phase for the purchase of digital medical equipment, to ensure that the procured equipment has adequate cybersecurity.
- Create a procurement process with defined roles, responsibilities, and decision-making authority. A dedicated role for safeguarding cybersecurity compliance in the procurement process should be considered.
- Include cybersecurity specific key performance indicators (KPI’s) to measure the efficiency of the procurement process.
- The clinic, ICT and medical technical department should cooperate closer, by creating a regular joint meeting for procurement planning. When the right stakeholders plan procurements together, it will contribute to lower costs since it increases the possibility of procuring equipment with adequate built-in security that does not have need for compensating security measures.
- Cooperate with other health regions to:
    - Acquire knowledge about best cybersecurity practices that might be currently unknown
    - Share information and knowledge that might benefit others
    - Discuss solutions
- Participate in meetings or forums with health sector specific vendors, to contribute raising the level of cybersecurity in digital medical equipment.
- Work towards standardization when it comes to procurement – that can contribute to increased security.
- Both people, processes and technology need to be considered in the procurement process to fully address all areas of cybersecurity

6.2 Recommendation for further research

This master’s thesis has focused primarily on the procurement process of digital equipment, and specifically on the procurement process of digital medical equipment in Norwegian hospitals. There are, however, three other phases in the lifecycle management of digital equipment that would be interesting to investigate as well:

- Operational phase – comes directly after the procurement phase and refers to the phase when equipment is put into use.
- Maintenance phase – overlaps with the operational phase to some degree, in the sense that they sometimes occur simultaneously. This phase refers to the regular

maintenance that equipment should undergo, to ensure that updates, patches, and similar, is installed to safeguard the confidentiality, integrity, and availability of data.

- Decommission phase – refers to the safe disposal of digital equipment that are discontinued and are at the end of their lifecycle.

Another recommendation for further research is to investigate the possibility, and implications, of implementing a national framework for procuring digital medical equipment that include important cybersecurity considerations. Alternatively, to investigate whether it is expedient to implement such a model.

Setting the right requirements and taking the right considerations helps to safeguard patient care. By ensuring that all health care institutions in Norway follow a set of minimum requirements, it will help to increase resilience to cybercriminals and cyberattacks.

References

ACRONIS. 2020. *The NHS cyber attack* [Online]. Available: https://www.acronis.com/en-eu/articles/nhs-cyber-attack/ [Accessed 28.03 2022].

BAREN, R. V. 2021. *The role of cybersecurity in hospital procurement processes* [Online]. Available: http://resolver.tudelft.nl/uuid:79b71f4a-034c-42cd-92a8-bf44a084eb7c [Accessed 29.04 2022].

BBC 1964. The Knowledge Explosion.

CENTER FOR INTERNET SECURITY 2019. CIS Controls v. 7.1. New York: Center for Internet Security.

CORONADO, A. J. & WONG, T. L. 2014. Healthcare Cybersecurity Risk Management: Keys To an Effective Plan. *Biomedical Instrumentation & Technology,* 48**,** 26-30.

DET KONGELIGE JUSTIS- OG BEREDSKAPSDEPARTEMENT. 2016. *Meld. St. 38: IKT-sikkerhet - et felles ansvar* [Online]. Available: https://www.regjeringen.no/contentassets/39c6a2fe89974d0dae95cd5af0808052/no/pdfs/stm201620170038000dddpdfs.pdf [Accessed 15.03 2022].

DEUSCHLER, M. 2020. *New guidance published for medical device and IVD cybersecurity under MDR and IVDR in Europe* [Online]. Available: https://www.emergobyul.com/blog/2020/01/new-guidance-published-medical-device-and-ivd-cybersecurity-under-mdr-and-ivdr-europe [Accessed 20.03 2022].

DIREKTORATET FOR E-HELSE. 2020. *Normen – Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren* [Online]. Available: https://www.ehelse.no/normen/normen-for-informasjonssikkerhet-og-personvern-i-helse-og-omsorgssektoren [Accessed 15.02 2022].

ENISA. 2020. *Procurement Guidelines for Cybersecurity in Hospitals* [Online]. Available: https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services/@@download/fullReport [Accessed 29.04 2022].

EUROPEAN COMMISSION. 2020. *MDCG 2019-16 - Guidance on Cybersecurity for medical devices* [Online]. Available: https://ec.europa.eu/docsroom/documents/41863 [Accessed 15.04 2022].

EVANS, S. 2016. *Cyberspace is New Domain for War: NATO* [Online]. Available: https://www.infosecurity-magazine.com/news/cyberspace-is-new-domain-for-war/ [Accessed 26.02 2022].

EVERETT, E. L. & FURSETH, I. 2019. *Masteroppgaven,* Oslo, Unversitetsforlaget.

FINKLE, J. 2016. *U.S. firm blames Russian 'Sandworm' hackers for Ukraine outage* [Online]. Available: https://www.reuters.com/article/us-ukraine-cybersecurity-sandworm-idUSKBN0UM00N20160108 [Accessed 30.11 2021].

FOOD AND DRUG ADMINISTRATION. 2014. *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices* [Online]. Available: https://www.fda.gov/media/86174/download [Accessed 15.04 2022].

FURULY, J. G. 2021. *Regjeringen: Datainnbruddet i Stortingets e-postsystem ble gjennomført fra Kina* [Online]. Available: https://www.aftenposten.no/norge/i/w8VXpG/regjeringen-datainnbruddet-i-stortingets-e-postsystem-ble-gjennomfoert [Accessed 13.03 2022].

GATLAN, S. 2020. *UHS restores hospital systems after Ryuk ransomware attack* [Online]. Available: https://www.bleepingcomputer.com/news/security/uhs-restores-hospital-systems-after-ryuk-ransomware-attack/ [Accessed 08.11 2021].

GATLAN, S. 2021. *Universal Health Services lost $67 million due to Ryuk ransomware attack* [Online]. Available: https://www.bleepingcomputer.com/news/security/universal-health-services-lost-67-million-due-to-ryuk-ransomware-attack/ [Accessed 06.11 2021].

GRØNMO, S. 2021. *Forskningsmetode - samfunnsvitenskap* [Online]. Available: https://snl.no/forskningsmetode_-_samfunnsvitenskap [Accessed 13.09 2021].

HALL, A. & PAYNE, S. 2018. *What is the IVDR?* [Online]. Available: https://www.phgfoundation.org/media/220/download/briefing-what-is-the-ivdr.pdf?v=1&inline=1 [Accessed 20.03 2022].

HELSE- OG OMSORGSDEPARTEMENTET. 2021a. *Medisinsk utstyr - en viktig del av helsearbeidet* [Online]. Available: https://www.regjeringen.no/no/tema/helse-og-omsorg/legemidler/innsikt/medisinsk-utstyr/id86835/ [Accessed 15.02 2022].

HELSE- OG OMSORGSDEPARTEMENTET. 2021b. *Sykehus* [Online]. [Accessed 13.01 2022].

HILL, K. 2012. *How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did* [Online]. Available: https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/?sh=5283e2546668 [Accessed 27.02 2022].

HOPE, A. 2020. *Ryuk Ransomware Attack Disrupts Universal Healthcare Services Operations Resulting in Ambulance Diversions and Alleged Deaths* [Online]. Available: https://www.cpomagazine.com/cyber-security/ryuk-ransomware-attack-disrupts-universal-healthcare-services-operations-resulting-in-ambulance-diversions-and-alleged-deaths/ [Accessed 06.11 2021].

HOULIHAN, J. W. 2019. *Lex Innocentium (697 AD): Adomnán of Iona – father of Western jus in bello* [Online]. Available: https://international-review.icrc.org/articles/lex-innocentium-697-ad-adomnan-iona-father-western-jus-bello [Accessed 20.11 2021].

HUANG, K., SIEGEL, M. & MADNICK, S. 2018. Systematically Understanding the Cyber Attack Business: A Survey. *ACM Computing Surveys.* Massachusetts: Massachusetts Institute of Technology.

HUMER, C. & FINKLE, J. 2014. *Your medical record is worth more to hackers than your credit card* [Online]. Available: https://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924 [Accessed 28.02 2022].

INFORMATION SECURITY FORUM. 2021. *Standard of Good Practice for Information Security 2020* [Online]. London: Information Security Forum. Available: https://www.securityforum.org/solutions-and-insights/standard-of-good-practice-for-information-security-2020/ [Accessed].

ISACA 2018. Introducing COBIT 2019 Executive Summary. Schaumburg: ISACA.

ISMS.ONLINE. 2020. *What is ISO 27001?* [Online]. Brighton: Alliantist Ltd Sussex Innovation Centre. Available: https://www.isms.online/iso-27001/ [Accessed].

JACOBSEN, D. I. 2015. *Hvordan gjennomføre undersøkelser?,* Oslo, Cappelen Damm Akademisk.

KAYE, D. 1995. *The importance of information* [Online]. Available: https://www.emerald.com/insight/content/doi/10.1108/EUM0000000003897/full/pdf?title=the-importance-of-information [Accessed 26.02 2022].

LOVDATA. 2014. *Forskrift om håndtering av medisinsk utstyr* [Online]. Available: https://lovdata.no/dokument/SF/forskrift/2013-11-29-1373 [Accessed 15.04 2022].

LYSNEUTVALGET. 2015. *NOU 2015:13 Digital sårbarhet - sikkert samfunn* [Online]. Available: https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf [Accessed 10.03 2022].

MARK, M. S., TØMTE, C., NÆSS, T. & RØSDAL, T. 2017. *IKT-sikkerhetskompetanse i arbeidslivet – behov og tilbud* [Online]. Available: https://nifu.brage.unit.no/nifu-xmlui/bitstream/handle/11250/2490041/NIFUrapport2017-32.pdf?sequence=6&isAllowed=y [Accessed 17.02 2019].

MELANOR. 2022. *Om oss* [Online]. Available: https://www.melanor.no/nb/om-melanor/ [Accessed 20.04 2022].

NASJONAL SIKKERHETSMYNDIGHET. 2022. *Risiko 2022* [Online]. Oslo: Nasjonal Sikkerhetsmyndighet. Available: nsm.no/Risiko2022 [Accessed 12.02 2022].

NATIONAL INSTITUTE FOR STANDARDS AND TECHNOLOGY. 2020. *Security and Privacy Controls forInformation Systems and Organizations* [Online]. Gaithersburg: National Institute for Standards and Technology. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf [Accessed].

NATO. 2021. *Cyber defence* [Online]. Brussel. Available: https://www.nato.int/cps/en/natohq/topics_78170.htm [Accessed 26.02 2022].

NORSIS. 2018. *Hackingen av Helse Sør-Øst – Oppsummering* [Online]. Available: https://norsis.no/hackingen-helse-sor-ost-oppsummering/ [Accessed 13.03 2022].

NORWEGIAN NATIONAL SECURITY AUTHORITY. 2020. *Grunnprinsipper for IKT-sikkerhet versjon 2.0* [Online]. Oslo: Norwegian National Security Authority. Available: https://nsm.no/getfile.php/133735-1592917067/Demo/Dokumenter/Veiledere/nsms-grunnprinsipper-for-ikt-sikkerhet-v2.0.pdf [Accessed].

NSD. 2022. *Create a data management plan* [Online]. Available: https://www.nsd.no/en/create-a-data-management-plan [Accessed 10.02 2022].

OTTERHOLT, E. 2021. *in vitro* [Online]. Available: https://sml.snl.no/in_vitro [Accessed 20.03 2022].

RABINOWITZ, J. 2018. *How Cybersecurity Factors into the Medical Device Procurement Process* [Online]. Available: https://blog.cybermdx.com/how-cybersecurity-considerations-should-factor-into-the-medical-device-procurement-process [Accessed 05.01 2022].

RIKSREVISJONEN. 2015. *Sak 3: Helseforetakenes ivaretakelse av informasjonssikkerhet i medisinsk-teknisk utstyr* [Online]. Oslo: Riksrevisjonen. Available: https://www.riksrevisjonen.no/globalassets/rapporter/no-2015-2016/helseforetakeneinformasjonssikkerhetutstyr.pdf [Accessed 09.01 2022].

RIKSREVISJONEN. 2020. *Undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer* [Online]. Available: https://www.riksrevisjonen.no/rapporter-mappe/no-2020-2021/undersokelse-av-helseforetakenes-forebygging-av-angrep-mot-sine-ikt-systemer/ [Accessed 10.01 2022].

RIKSREVISJONEN. 2022. *About us* [Online]. Available: https://www.riksrevisjonen.no/en/about-the-oag/about-us/ [Accessed 09.01 2022].

RIOS, B. 2015. Cybersecurity Expert: Medical Devices Have 'A Long Way to Go'. *Biomedical Instrumentation & Technology,* 49**,** 197-200.

ROSTAD, I. L., SKEIE, T., ANDREASSEN, R., FORLAND, G. & PEDERSEN, L. 2022. *Datainnbrudd mot ambulanser på flere sykehus i Nord-Norge: – Et alvorlig datainnbrudd* [Online]. Available: https://www.nrk.no/tromsogfinnmark/helse-nord_-datainnbrudd-pa-flere-sykehus-i-nord-norge-1.15926897 [Accessed 09.04 2022].

SCHJØLBERG, S. 2017. *Cyberkriminalitet,* Oslo, Universitetsforlaget.

SCHWARTZ, S., ROSS, A., CARMODY, S., CHASE, P., COLEY, S. C., CONNOLLY, J., PETROZZINO, C. & ZUK, M. 2018. The Evolving State of Medical Device Cybersecurity. *Biomedical Instrumentation & Technology,* 52**,** 103-111.

SIPILÄ, J. 2020. *https://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924* [Online]. Available: https://edition.cnn.com/2020/10/27/tech/finland-therapy-patients-blackmailed-data-breach-intl/index.html [Accessed 28.02 2022].

ST. OLAVS HOSPITAL. 2022. *Medisinsk teknisk avdeling* [Online]. Available: https://stolav.no/avdelinger/divisjon-st-olavs-driftsservice/medisinsk-teknikk#hva-er-medisinsk-teknisk-utstyr-mtu [Accessed 15.02 2022].

STATISTISK SENTRALBYRÅ. 2016. *Døgnopphold, liggedager og gjennomsnittlig liggetid ved somatiske sykehus, etter kjønn (SÅ 134)* [Online]. Available: https://www.ssb.no/304492/dognopphold-liggedager-og-gjennomsnittlig-liggetid-ved-somatiske-sykehus-etter-kjonn-sa-134 [Accessed 13.03 2022].

SYKEHUSINNKJØP. 2021. *Oppdragsdokument 2021* [Online]. Available: https://sykehusinnkjop.no/Documents/Om%20oss/Om%20oss%20dokumenter/Oppdragsdokument%20Sykehusinnkj%C3%B8p%20HF%202021.pdf [Accessed 15.01 2022].

SYKEHUSINNKJØP. 2022. *Om oss* [Online]. Available: https://sykehusinnkjop.no/om-oss [Accessed 31.03 2022].

TJORA, A. 2020. *Kvalitative forskningsmetoder i praksis,* Oslo, Gyldendal.

US DEPARTMENT OF DEFENSE. 2011. *Department of Defense Strategy for Operating in Cyberspace* [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf [Accessed 26.02 2022].

UTENRIKSDEPARTEMENTET. 2021. *Datainnbruddet i Stortingets e-postsystem* [Online]. Available: https://www.regjeringen.no/no/dokumentarkiv/regjeringen-solberg/aktuelt-regjeringen-solberg/ud/pressemeldinger/2021/pm_datainnbrudd/id2866410/ [Accessed 13.03 2022].

WHITE, G. 2009. Strategic, tactical, & operational management security model. *Journal of Computer Information Systems,* 49**,** 71-75.

Attachments

Initial email to health regions and hospitals

Hei!

Jeg tar kontakt med dere i forbindelse med min masteroppgave som jeg holder på å skrive ved NTNU for å fullføre min grad innen cybersikkerhet nå i 2022.

Masteroppgaven omhandler innkjøpsprosessen av digitalt medisinsk utstyr, der jeg ønsker å undersøke hvilke cybersikkerhetshensyn som tas i innkjøpsprosessen av slikt utstyr. For å besvare oppgaven er jeg avhengig av å intervjue noen som kjenner godt til innkjøpsprosessen og hvilke avveininger og vurderinger som tas der. Intervjuet er estimert til å ta rundt 60 minutter, men kan ta kortere tid om intervjudeltaker har fått anledning til å gå igjennom spørsmålene på forhånd (spørsmålene sendes til intervjudeltaker god tid i forveien). Intervjuet blir gjennomført på Teams, og med opptak for senere transkripsjon. Besvarelsene vil bli håndtert iht. retningslinjer fra Norsk Senter for Forskningsdata, og personopplysninger vil bli anonymisert. Etter at oppgaven er skrevet ferdig, vil opptakene slettes permanent.

I første omgang ønsker jeg å komme i kontakt med noen som kan bistå med denne datainnsamlingen, de vil få tilsendt et samtykkeskjema + ytterligere informasjon om hvordan intervjuene blir gjennomført og dataen behandlet.

Håper dette er noe dere har anledning til å hjelpe meg med!

Med vennlig hilsen

Erik Stol Øyan

Interview guide

Studie ved NTNU, Institutt for informasjonssikkerhet og kommunikasjonsteknologi, våren 2022.

Hvor samkjørte er norske sykehus med velkjente cybersikkerhetsrammeverk når det kommer til cybersikkerhetsavveininger som tas i innkjøpsprosessen av digitalt medisinsk utstyr?

Praktisk informasjon

- **Varighet**: intervjuet er estimert til å ta omtrent 60 minutter, avhengig av deltagerens forberedelse, og består av til sammen sju -7- spørsmål.
- **Gjennomføring**: intervjuet gjennomføres på Teams (e.l.), og vil tas opp for transkribering i etterkant. Så fort transkribering er fullført, vil opptaket slettes.

Studien vil anonymiseres, slik at potensielle sårbarheter eller svakheter som avdekkes i intervjusammenheng ikke blir avslørt og kan utnyttes av utenforstående eller cyberkriminelle.

Intervjuspørsmål

- Spørsmål 1 – bakgrunnsinformasjon: beskriv din rolle i innkjøpsprosessen

- Spørsmål 2 – hvordan vurderes cybersikkerhet i anskaffelsesfasen av digitalt medisinsk utstyr?
- Spørsmål 3 – er det noen rammeverk eller «beste praksiser» som følges i anskaffelsesfasen av digitalt medisinsk utstyr?
- Spørsmål 4 – hvilke interessenter er vanligvis involvert i anskaffelsesfasen av digitalt medisinsk utstyr?
- Spørsmål 5 – har noen av disse interessentene cybersikkerhetskompetanse?
- Spørsmål 6 – basert på din erfaring, hva mener du kan og/eller bør gjøres for å forbedre cybersikkerheten i anskaffelsesprosessen?
- Spørsmål 7 – hvordan sikrer dere at cybersikkerhetshensynene i anskaffelsesprosessen blir fulgt?