Integrating Cybersecurity into Medical Device Procurement

A Comparative Case Study of Dutch Hospitals

Integrating Cybersecurity into Medical Device Procurement

A Comparative Case Study of Dutch Hospitals

By

E.R.W. (Ewoud) Cornelissen
5814286

in partial fulfilment of the requirements for the degree of

Master of Science
in Complex Systems Engineering and Management

at the Delft University of Technology, Faculty of Technology, Policy, and Management,
to be defended publicly on Wednesday July 3rd, 2024, at 10:00.

Chairperson:	Dr. S. (Saba) Hinrichs-Krapels	
First supervisor:	Dr. R.S. (Rolf) van Wegberg	TU Delft, Section O&G
Second supervisor:	Dr. S. (Saba) Hinrichs-Krapels	TU Delft, Section PA
Advisor:	L.F. (Lorenz) Kustosch,	TU Delft, Section O&G

An electronic version of this thesis is available at http://repository.tudelft.nl/.
Front page image credits: Image ID 37133261 on https://vectorstock.com/.

Preface

This thesis is the culmination of my academic journey in Complex Systems Engineering and Management at the TU Delft. The work presented here represents not only the knowledge and skills I have acquired throughout my studies but also the end of a thrilling and enriching period in my life.

The process leading up to this thesis was filled with ups, downs, learning, and growth. This wasn't possible without the support and help of several individuals.

First, I would like to start by extending my gratitude to my first supervisor, Rolf van Wegberg. Our first contact was in May 2023 already. During this crucial initial phase your critical questions and guidance pointed me towards a topic I was passionate about, which ultimately resulted in me enjoying the research process to the fullest. Additionally, your feedback and cool-headedness proved crucial to me at times when I was stuck. Second, I would like to thank my second supervisor Saba Hinrichs-Krapels for your willingness to put me in contact with several relevant stakeholders and for your critical and precise feedback, which contributed significantly to the end result. Third, I am forever grateful to my advisor, Lorenz Kustosch. For the both of us this thesis was a first: for me writing it, and for Lorenz guiding it. However, I could not have wished for a more involved and caring advisor. Our weekly meetings would always lift me up, even when I was a bit stuck on certain topics, and your feedback and critical thoughts were crucial for shaping my thesis as it is now. Based on your progress in Dutch class, it should be easy for you to read this: dank je wel!

I would also like to thank all interviewees who participated in this thesis. Your willingness to contribute time and knowledge made this thesis possible and proved extremely valuable.

Finally, I would like to thank my family, and friends for their support, contacts, and encouragement. Your belief in me motivated me throughout my academic career.

This thesis is dedicated to my father. I am extremely grateful that you are still here to celebrate the end of my academic journey and the start of my professional career.

I hope that the findings and discussions presented here will contribute to the ongoing discussions on cybersecurity in healthcare and inspire future research and discovery.

Ewoud Cornelissen
Delft, 2024

[This page is left blank intentionally]

Summary

This thesis examines the procurement practices of medical devices in Dutch hospitals with a focus on how cybersecurity considerations are incorporated. With the increasing connectivity of medical devices, cybersecurity risks have become a critical concern for Dutch hospitals. Cyberattacks on medical devices can directly impact patient safety and data security. This research aims to highlight the importance of integrating cybersecurity considerations into the procurement process to mitigate these risks from the start. The findings are expected to enhance patient safety, inform policy and regulatory frameworks, and contribute to building a more resilient healthcare system.

Research goal and questions

The goal of this thesis is to map the procurement practices of Dutch hospitals through a socio-technical lens, in line with the CoSEM programme. Therefore, not only the technical aspects of cybersecurity are considered, but also the regulatory, economic and human factors in line with the complex nature of a decision-making process. To extent the broad view of this thesis to the human factors, stakeholders from both within the hospital and outside are considered. Finally, the aim of this thesis is to contribute scientifically to the domain of process analyses, specifically procurement processes in the context of Dutch hospitals, and to provide recommendations to Dutch hospitals to improve the role of cybersecurity. Therefore, this thesis is guided by the following main research question:

To what extent are cybersecurity considerations integrated into the procurement process of medical devices in Dutch hospitals?

To be able to answer this main research question, the following five sub questions were used to guide this research:

1. *How are cybersecurity considerations included in the current regulations and standards governing medical devices and the procurement thereof?*
2. *What are the existing general procurement practices for medical devices in hospitals in The Netherlands?*
3. *What is the effect of external stakeholders on the procurement process of medical devices in the context of cybersecurity?*
4. *How are cybersecurity aspects considered compared to other considerations during the procurement of new medical devices?*
5. *What recommendations can be derived to improve the role of cybersecurity during the procurement process of new medical devices in Dutch hospitals, if at all?*

Research approach and methods

First, research was conducted through a comprehensive literature review to define the research problem and identify knowledge gaps, followed by desk research to gain an overview of existing regulation surrounding cybersecurity and procurement in hospitals, and scientific research related to procurement and cybersecurity in hospitals. Semi-structured interviews were then conducted with key stakeholders involved in the procurement process in three Dutch hospitals, and a cybersecurity specialist. Data from these interviews were analysed using a framework analysis to identify key themes and stakeholder dynamics. This framework analysis then allowed to synthesise the findings into a comparative case study, with each hospital analysed as a separate case. This approach allows to identify differences and similarities between the hospitals' approach to procurement and cybersecurity, which in return allows for a general view on the procurement processes in Dutch hospitals. Finally, these findings were used to define practical recommendations for enhancing cybersecurity in medical device procurement.

Key findings

To answer the first sub question, this thesis examines European Union and Dutch regulations but also considers international policies due to the global nature of medical device manufacturing. The following relevant regulations were found: the EU's medical device regulation, network and information security directive, the general data protection regulation, the Dutch NEN7510 norm, and the US's FDA rules and HIPAA act. From the analysis of these regulations, it can be concluded that their main focus lies on setting minimum requirements for medical device cybersecurity, rather than setting standards for the procurement process.

Second, semi-structured interviews with participants from several hospitals concluded that the procurement process across these hospitals show a striking resemblance. The procurement steps can be defined as follows:

1. **Market exploration:** An initial exploration is performed to identify potential providers and projected costs.
2. **Business case and financial check:** A business case has to be made, explaining why a device should be procured and the benefits it proposes. This case is then presented to some sort of an investment committee, which can approve it and allocate funds
3. **Program of requirements:** A wide variety of stakeholders, all with a different expertise, are requested to set requirements for the new device, bases on their background.
4. **Market exploration:** After the program of requirements is set, a second market exploration is performed to identify the different suppliers that could adhere to it.
5. **Offer request and evaluation:** Suppliers are requested to fill in how they adhere to the program of requirements together with an offer. These filled in program of requirements and offers are then evaluated by all stakeholders that contributed earlier.
6. **Device on trial:** As an optional extra step, a device could be installed on a trial basis, before a final decision is made.
7. **Final decision in consultation:** A final decision is made in consultation with all participating internal stakeholders.
8. **Contract negotiation:** Contracts are negotiated with the selected supplier. This includes aftersales services and the price.
9. **Evaluation:** Sometimes, the procurement processes or supplier satisfaction are evaluated afterwards so that procurement processes can be improved.

During this process, a wide variety of internal stakeholders have to work together. This can sometimes lead to a discrepancy between the different stakeholders, who might have a different view on the importance of some requirements. However, a consensus is always reached as the final decision is made in consultation with everyone involved.

Third, several external influences on the procurement process were noted. Manufacturers play a significant role by engaging with doctors, promoting their devices, and maintaining long-term relationships with hospitals, often providing trial installations which could influence decisions. Medical conferences act as venues for manufacturers to showcase new devices and facilitate networking among medical professionals, which can affect procurement choices. Doctors from different hospitals also influence each other by sharing their experiences and opinions about various devices. In the context of this thesis, cybersecurity specialists were also considered a potential influence on the procurement process of medical devices. However, their influence is limited, as they mainly function as a linking pin between hospitals to share their experiences.

Finally, a theoretical lens was synthesised to define the role of cybersecurity during the procurement process. This theoretical lens and the interviews showed that, whilst cybersecurity is considered important, it tends to be viewed more as a baseline criterium rather than a decisive factor in the decision-making process. Hospitals tend to prioritise functionality, compatibility, and cost over cybersecurity, which is often perceived as a compliance element. The cybersecurity requirements set are shaped by internal policies and external regulations which were mentioned earlier. However, it does not significantly drive procurement decisions.

Recommendations for hospitals

The main recommendation that this thesis provides is the need for cybersecurity awareness training for all stakeholders involved in the procurement process. Currently, there is a disparity in the understanding of cybersecurity's significance within hospitals and the procurement process. The recommendation stemming from this study is clear: by cultivating a shared understanding of the threats posed by cyber-attacks among all stakeholders, hospitals can elevate the prioritisation of cybersecurity measures during the procurement process.

In addition to this main recommendation, several other recommendations are given. First, higher management could be included more during the procurement process to align all participating stakeholders during the procurement process on the importance of cybersecurity. This also aligns with the NIS2 directive of the EU. Second, the MedTech department and IT department increasingly must work together due to the digitalisation of medical devices. To align their processes better and to provide a singular view on cybersecurity during the procurement process, these two departments could merge. Finally, sometimes procurement processes and suppliers are evaluated, which are used in future procurement processes. Cybersecurity of devices could also be evaluated, either by the hospital itself or a third-party. This evaluation can then be used to motivate cybersecurity requirements in future procurement processes.

Limitations and future research recommendations

This thesis outlines several potential future research avenues. First, research could explore how compliance with tender law affects procurement in academic hospitals and the role cybersecurity plays in these processes. Furthermore, future studies could investigate manufacturers' perspectives on cybersecurity's importance, the adequacy of current regulations, and their views on collaborative efforts with healthcare institutions to enhance cybersecurity. Third, instead of focussing on multiple hospitals as is the case with this thesis, a case study approach could examine different stakeholders' attitudes towards cybersecurity within a single hospital, exploring their priorities, perceived trade-offs between cybersecurity measures and operational efficiency, and potential strategies to reconcile these differences. Fourth, research could compare how EU regulations impact procurement and cybersecurity in hospitals across different countries, identifying common challenges and disparities. Finally, the effects of NIS2 on the procurement processes in Dutch hospitals could be studied, focusing on changes post-transposition into Dutch law, how hospitals assess the cybersecurity of their suppliers, and the involvement of management bodies in procurement.

The limitations of this study include its reliance on qualitative data, which may introduce subjectivity and bias, especially since this thesis written by only one author. In addition, this thesis is based upon a small number of semi-structured interview, with a total of seven. This affects the generalisability of this thesis to the whole of the Netherlands.

Conclusion

This study highlights the critical need for integrating robust cybersecurity measures into the procurement processes of medical devices. By adopting the provided recommendations, hospitals can significantly enhance their procurement practices, ensuring the safety and security of medical devices and protecting patient health and data. This executive summary aims to equip scientists and healthcare professionals with a comprehensive understanding of the procurement process in Dutch hospitals and the importance of cybersecurity in healthcare, ultimately contributing to the development of more secure and efficient healthcare systems. Integrating cybersecurity into medical device procurement will fortify healthcare systems against an ever-evolving landscape of cyber threats.

[This page is left blank intentionally]

List of Acronyms

CDM	Complex Decision-Making
CE	Conformité Européene
CERT	Computer Emergency Response Team
CIA	Confidentiality, Integrity, and Availability
CIPS	Chartered Institute of Procurement & Supply
CoSEM	Complex Systems Engineering and Management
CSIRT	Computer Security Incident Response Team
CVD	Coordinated Vulnerability Disclosure
DPIA	Data Protection Impact Assessment
ENISA	European Union Agency for Cybersecurity
e-PHI	Electronic Protected Health Information
EU	European Union
FDA	Food and Drug Administration
GDPR	General Data Protection Regulation
HDO	Healthcare Delivery Organisation
HHS	U.S. Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
HREC	Human Research Ethics Committee
IMDRF	International Medical Device Regulators Forum
IRP	Incident Response Plan
IT	Information Technology
MDCG	Medical Device Coordination Group
MDD	Medical Devices Directive
MDR	Medical Devices Regulation
MedTech	Medical Technology
MRQ	Main Research Question
NCSC	Nationaal Cyber Security Centrum
NIS	Network and Information Security Directive
NIS2	Network and Information Security 2 Directive
PPM	Push-Pull-Mooring
SPDF	Secure Product Development Framework
SQ	Sub Question
TPLC	Total Product Life Cycle
US	United States
VPN	Virtual Private Network
WHO	World Health Organization

List of Tables

List of Figures

[This page is left blank intentionally]

Contents

1 Introduction

In the healthcare sector, there has been a significant surge in cyber-attacks. Next to this, methods employed have evolved significantly, thanks to the adoption of more sophisticated techniques (Jalali et al., 2019). This trend is linked to the increasing use of advanced, interconnected technologies, such as imaging and patient monitoring equipment, to enhance patient care in hospitals (Bhosale et al., 2021). However, the integration of these interconnected technologies introduces numerous cybersecurity risks to a hospitals' Information Technology (IT) infrastructure (Ahmed & Barkat Ullah, 2018). Next to this, when more systems become connected, the security risks increase even more, leading to a hospital that is exposed to data breaches (McLeod & Dolezel, 2018). These risks are introduced to a critical sector which already is one the primary targets for cyber-attacks (Coventry & Branley, 2018). Yet, research suggests that security and privacy policies have not scaled accordingly (Uwizeyemungu et al., 2019).

Although there are many different types of cyber-attacks, hospitals are specifically susceptible to ransomware attacks (Ponemon Institute, 2023). Cyber-attacks targeting hospitals pose significant risks to society, impacting both the social and physical lives of people (Ratta et al., 2021). For instance, malicious actors could focus on patient records, which often contain sensitive information substantial enough to facilitate identity theft, financial fraud, or even passport applications (Coventry & Branley, 2018). Additionally, interconnected medical devices used within hospitals can be hacked, potentially resulting in the administration of fatal doses of medication to patients (Klonoff, 2015). While independent hackers will most likely not see the advantage of this, they could be leveraged by nation-state actors during periods of heightened geopolitical tensions (Coventry & Branley, 2018). Furthermore, when interconnected medical devices are poorly configured, they can be used as an entry point to a hospital's IT network (Forescout Research Labs, 2020). These instances represent just a glimpse of the large number of threats confronting hospital computer networks (Bhosale et al., 2021; Coventry & Branley, 2018; Jalali et al., 2019).

The security of interconnected technologies within hospitals has not gone unnoticed by regulatory bodies. For example, the PATCH act mandates the Food and Drug Administration (FDA) in the U.S. to require manufactures of medical devices to continuously develop security fixes to address critical vulnerabilities (PATCH Act of 2022, 2022). In the European Union, interconnected medical devices are regulated by the Medical Device Regulation (MDR), which includes the notion that devices should continue to be operable in the case of any attack (Ludvigsen, 2023).

Nevertheless, research indicates that these regulations frequently impose minimal requirements on manufacturers as they strive to keep costs low (Ludvigsen, 2023; Zou & Mehta, 2023). This results in a discrepancy in the cybersecurity approach adopted by different device manufacturers, with some prioritizing the development of robust platforms while others opt for cost reduction (Lam & Wong, 2018). Hence, procurement in hospitals can play a vital role in enhancing the cybersecurity of hospital IT systems, as the medical devices procured are an integral part of and potential gateway to the hospital's infrastructure. This is also stressed by an article published by Dark Reading, a cybersecurity trade magazine (Dark Reading, n.d.; Zou & Mehta, 2023). When insecure interconnected medical devices are acquired and integrated into a hospital, they could negatively affect the overall system security. Conversely, the integration of security-oriented interconnected medical devices will not negatively affect the security of the system, as it is only as strong as its weakest link.

This problem is also described by industry reports such as by Claroty & Team82 (2024) on the state of medical device cybersecurity. They stress that regulations focus too much on data privacy, instead of cybersecurity. This was sufficient at the time of introduction of these regulations, but as devices have evolved and have become more connected, the focus of cybercriminals is expected to shift to disrupting hospital operations. As a result, 63% of known exploited vulnerabilities in computer systems are found on hospital networks, highlighting the ongoing issue of inadequate patching systems. To counteract this, Claroty & Team82 (2024) calls for cybersecurity to be a proactive exercise instead of reactive, for hospitals and manufacturers alike.

Therefore, this thesis will focus on the procurement of medical devices in hospitals and how cybersecurity is considered during this process. The rest of this introduction will discuss relevant definitions of concepts used in this research, as well as the research gap, scope, relevance, and main research question (MRQ).

1.1 Definitions

To have a clear understanding throughout this thesis of what is meant by procurement, a medical device, and cybersecurity, this section will define these concepts.

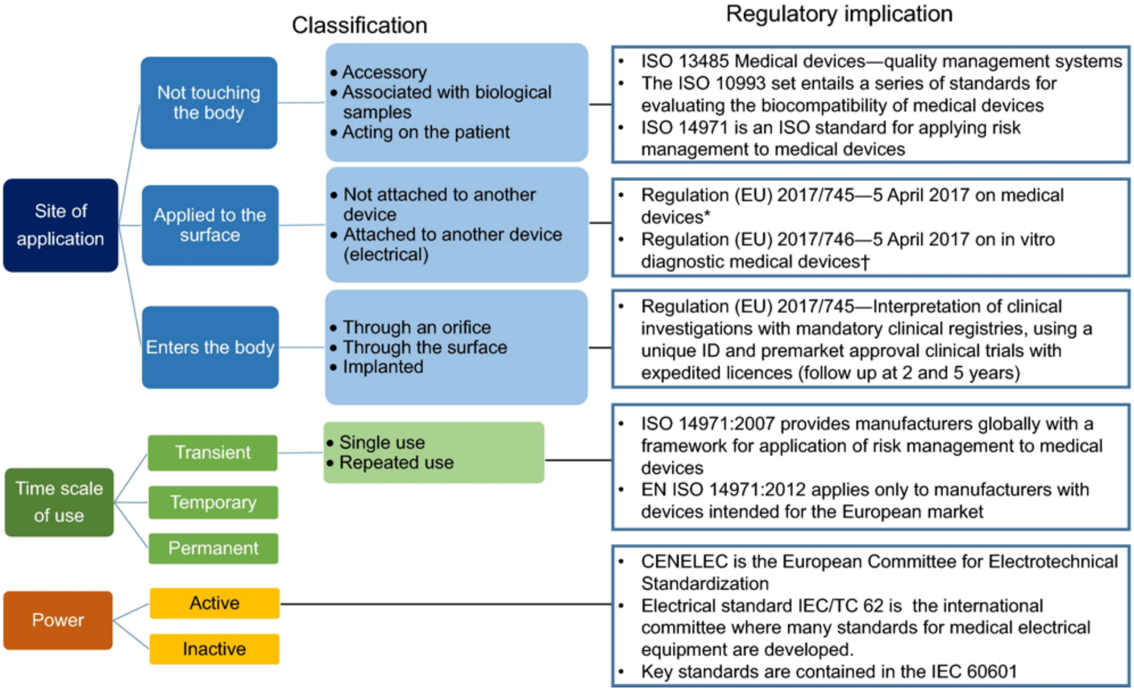
1.1.1 Procurement definition

Various definitions of procurement are found across different sectors and fields, resulting in ambiguity that can lead to unwanted implications (Prier & Mccue, 2009). Therefore, it is essential to establish a clear understanding of procurement before conducting a literature review, ensuring alignment among the included articles. While numerous definitions of procurement exist, this study will follow the definition provided by the Chartered Institute of Procurement & Supply (CIPS) due to their expertise on the topic. CIPS (n.d.) defines procurement as follows: "the buying of goods and services that enable an organisation to operate its supply chains, in a profitable and ethical manner". Notably, this definition is not only used due to CIPS' expertise but is also deemed suitable for the healthcare sector by Turrell (2014). Therefore, this definition will be used throughout this study.

1.1.2 Medical device definition

A medical device can be defined in many ways. However, this can lead to many interpretations of this research and the articles that will be included in this literature review. Therefore, this section will focus on defining the definition of a medical device for this study.

Legislative bodies, such as the EU, all have their own definitions of a medical device. However, these are also not univocally interpreted (Racchi et al., 2016). Therefore, this study will follow the definition set out by Aronson et al. (2020). They define a medical device as follows: "A contrivance designed and manufactured for use in healthcare, and not solely medicinal or nutritional" (Aronson et al., 2020, p. 89). In addition, they propose classifications for medical devices as depicted in Figure 1 below.



- ISO 13485 Medical devices—quality management systems
- The ISO 10993 set entails a series of standards for evaluating the biocompatibility of medical devices
- ISO 14971 is an ISO standard for applying risk management to medical devices

- Regulation (EU) 2017/745—5 April 2017 on medical devices*
- Regulation (EU) 2017/746—5 April 2017 on in vitro diagnostic medical devices†

- Regulation (EU) 2017/745—Interpretation of clinical investigations with mandatory clinical registries, using a unique ID and premarket approval clinical trials with expedited licences (follow up at 2 and 5 years)

- ISO 14971:2007 provides manufacturers globally with a framework for application of risk management to medical devices
- EN ISO 14971:2012 applies only to manufacturers with devices intended for the European market

- CENELEC is the European Committee for Electrotechnical Standardization
- Electrical standard IEC/TC 62 is the international committee where many standards for medical electrical equipment are developed.
- Key standards are contained in the IEC 60601

Figure 1 - Medical device classifications (Aronson et al., 2020)

However, this study will exclude transient and inactive devices, as they are unlikely to be integrated into a central IT infrastructure. One addition made to the definition of a medical device by Aronson et al. (2020), is that it will be required to be interconnected. In addition, the medical device must be, or will be, included within a hospital's IT infrastructure. Otherwise, cybersecurity will most likely not play a significant role in the procurement of a new medical device.

1.1.3 Cybersecurity

A wide variety of definitions exist for the term 'cybersecurity' or 'cyber security'. However, as cybersecurity is the focal point of this thesis, a singular definition is needed. Craigen et al. (2014) define cybersecurity as follows: "*The organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights.*" Additionally, Schatz et al. (2017) provide another definition of cybersecurity: "*The approach and actions associated with security risk management processes followed by organisations and states to protect confidentiality, integrity and availability of data and assets used in cyber space. The concept includes guidelines, policies and collections of safeguards, technologies, tools and training to provide the best protection for the state of the cyber environment and its users.*" Finally, the European Union Network and Information Security Agency (ENISA) links cybersecurity to the concept of cyberspace and defines it as follows: "[*The] security of cyberspace, where cyberspace itself refers to the set of links and relationships between objects that are accessible through a generalised telecommunications network, and to the set of objects themselves where they present interfaces allowing their remote control, remote access to data, or their participation in control actions within that cyberspace"* (Brookson et al., 2016).

Although attacks related to data are the most common in the healthcare sector (Ponemon Institute, 2023), the adverse effects of poor cybersecurity can be much broader than that (Bhosale et al., 2021; Coventry & Branley, 2018; Jalali et al., 2019). Therefore, a broad definition for cybersecurity is also required. To achieve this, the definitions provided above are combined to form the following definition of cybersecurity used throughout this thesis:

Guidelines, policies, and collections of safeguards, technologies, tools and training to protect cyberspace, cyberspace-enabled systems and its users, where cyberspace itself refers to the links and relations between objects that are accessible through a generalised telecommunications network.

1.2 Knowledge gap

To identify an appropriate knowledge gap, a literature review has been performed. This section will discuss the methods that were used, as well as the results.

1.2.1 Literature review process

A systematic search was performed on February 21st, 2024, using Scopus to retrieve relevant articles. Scopus was chosen for its extensive coverage across various disciplines (Pranckutė, 2021). Initially, the search query "cyber* AND procurement AND (hospital* OR healthcare)" was used to closely align with the intended research focus. However, this returned only eight results, deemed insufficient for a comprehensive literature review, though it is a first hint at a research gap. As searching for specific cybersecurity considerations resulted in too little articles, the approach was chosen to expand the search scope to procurement in hospitals in general. Thereby, a general overview of different considerations during the procurement of medical devices can be created. Therefore, the search query "(procur* OR purchas*) AND hospital* AND proces*" was used, resulting in 4,237 articles.

The initial article selection involved database filtering. Firstly, publication dates were limited to the past decade (2014-2024) to capture recent developments, including the surge in hospital cyber-attacks during the COVID-19 pandemic (Minaar & Herbig, 2021). Secondly, the results were refined to encompass articles, reviews, conference papers, and book chapters, excluding other publication types deemed less relevant. Thirdly, publications were limited to be in English and Dutch, as to align with the reviewer's proficiency, resulting in a total of 1,399 documents.

Following the selection process, screening took place by exporting the search results from Scopus and examining them by a single reviewer. Titles were initially screened to ensure relevance to procurement processes in the healthcare sector, leading to the exclusion of 1,318 articles. Second, abstracts were assessed to identify articles mentioning the procurement of medical devices in hospitals aligned with the definitions given in section 1.1, resulting in the exclusion of 60 articles. Third, full-text examination took place to verify again if the literature discusses procurement of medical devices, aligned with the definition given earlier. Additionally, the inclusion in the literature of considerations made during the procurement process was considered, resulting in the exclusion of an additional eight articles which did not adhere to these inclusion criteria. Consequently, a total of 14 articles remained. Finally, forward snowballing was used to find citations to these 14 articles, as to include more recent studies on the topic (Wee & Banister, 2016). After applying the same filters as mentioned in the previous paragraph, four additional articles were included. As a result, 18 articles are included in this review, which are detailed in Table 1, with the entire search process summarized in Figure 2.

Table 1 - Articles included in the literature review

No.	*Authors*	*Title*	*Year*	*Published in*	*Document type*
1	Herrero et al.	Prioritizing Patient Safety: Analysis of the Procurement Process of Infusion Pumps in Spain	2023	International Journal of Environmental Research and Public Health	Article
2	Martin et al.	Hospital-based health technology assessment of innovative medical devices: insights from a nationwide survey in France	2023	International Journal of Technology Assessment in Health Care	Article
3	Filiniuk et al.	Current Approaches of Health Technologies Introduction in Ukrainian Hospitals	2023	ScienceRise: Pharmaceutical Science	Article
4	Brito Fernandes et al.	Citizen engagement in healthcare procurement decision-making by healthcare insurers: recent experiences in the Netherlands	2022	Health Research Policy and Systems	Article
5	Rahmani et al.	Comparative Study of Medical Equipment Procurement in Selected Countries	2022	Medical Journal of the Islamic Republic of Iran	Article
6	Hinrichs-Krapels et al.	Purchasing high-cost medical devices and equipment in hospitals: A systematic review	2022	BMJ Open	Article
7	Bosmans et al.	Procurement, commissioning and QA of AI based solutions: An MPE's perspective on introducing AI in clinical practice	2021	Physica Medica	Article
8	Boulding & Hinrichs-Krapels	Factors influencing procurement behaviour and decision-making: an exploratory qualitative study in a UK healthcare provider	2021	BMC Health Services Research	Article
9	Rahmani et al.	Value-Based procurement for medical devices: A scoping review	2021	Medical Journal of the Islamic Republic of Iran	Article
10	Callea et al.	Integrating HTA Principles into Procurement of Medical Devices: The Italian National HTA Programme for Medical Devices	2020	IFMBE Proceedings	Conference paper
11	Blüher et al.	Critical Review of European Health-Economic Guidelines for the Health Technology Assessment of Medical Devices	2019	Frontiers in Medicine	Article
12	Miller et al.	How Procurement Judges The Value of Medical Technologies: A Review of Healthcare Tenders	2019	International Journal of Technology Assessment in Health Care	Article
13	Priestman et al.	Lessons learned from a comprehensive electronic patient record procurement process - Implications for healthcare organisations	2019	BMJ Health and Care Informatics	Article
14	Vincent & Blandford	How do health service professionals consider human factors when purchasing interactive medical devices? A qualitative interview study	2017	Applied Ergonomics	Article
15	Callea et al.	The impact of HTA and procurement practices on the selection and prices of medical devices	2017	Social Science and Medicine	Article

16	Lingg et al.	Attitudes of orthopedic specialists toward effects of medical device purchasing	2017	International Journal of Technology Assessment in Health Care	Article
17	Lingg et al.	Effects of procurement practices on quality of medical device or service received: A qualitative study comparing countries	2016	BMC Health Services Research	Book chapter
18	Billaux et al.	Innovative medical devices and hospital decision making: A study comparing the views of hospital pharmacists and physicians	2016	Australian Health Review	Article

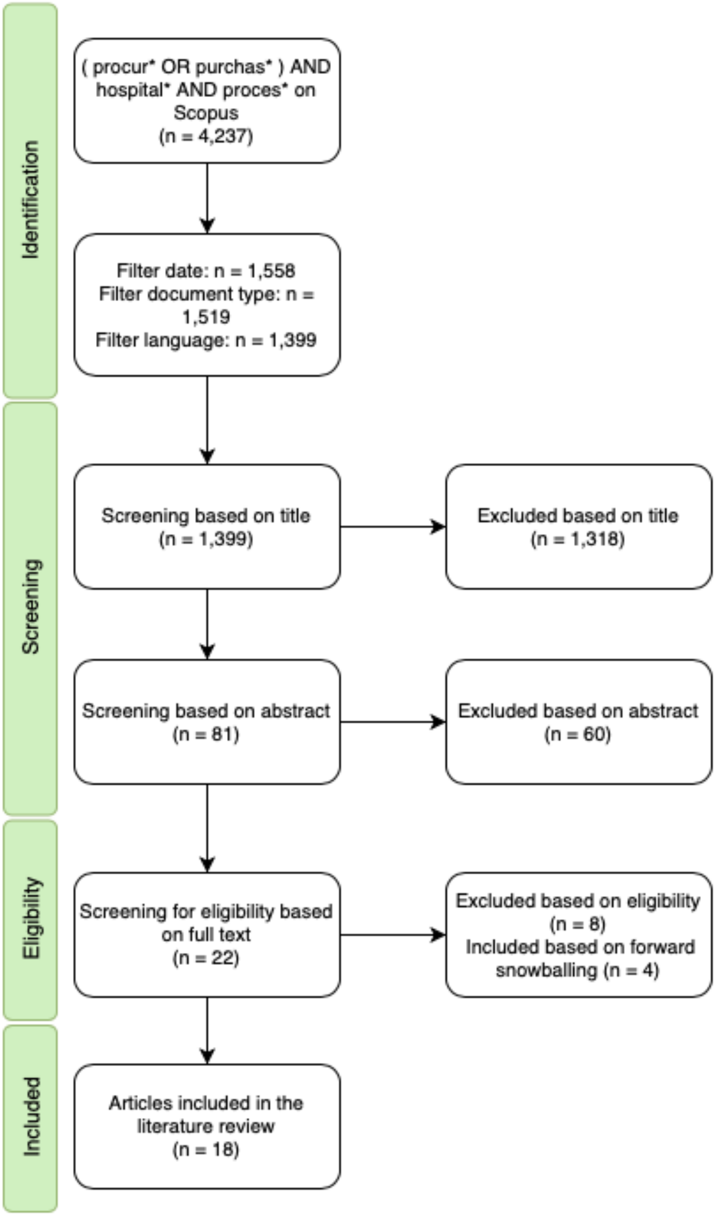

Identification
(procur* OR purchas*) AND hospital* AND proces* on Scopus (n = 4,237)
Filter date: n = 1,558
Filter document type: n = 1,519
Filter language: n = 1,399
Screening
Screening based on title (n = 1,399)
Excluded based on title (n = 1,318)
Screening based on abstract (n = 81)
Excluded based on abstract (n = 60)
Eligibility
Screening for eligibility based on full text (n = 22)
Excluded based on eligibility (n = 8)
Included based on forward snowballing (n = 4)
Included
Articles included in the literature review (n = 18)

Figure 2 - Flow diagram visualising search strategy

1.2.2 Discussion

The examination of each paper aimed to identify various factors considered during the procurement of new medical devices. A total of 14 considerations were documented in the literature. These encompassed diverse elements such as device costs (Callea et al., 2017), end user preferences - such as those expressed by clinicians or nurses (Filiniuk et al., 2023) - and compatibility with a hospital's existing IT infrastructure or operational processes (Martin et al., 2023). It is noticeable that all but one paper mentioned the significance of economic factors in procurement, a perspective that seems logical in an industry with already high costs. Following closely, the second most frequently cited factor was related to the physical or technical specifications that medical devices must meet. For instance, requirements such as possessing a CE (Conformité Européene) mark (Vincent & Blandford, 2017), or maintaining low noise levels (Herrero et al., 2023) were highlighted. While some factors were mentioned less frequent, only three were mentioned once. This means that 11 factors have been validated by more than one piece of literature. All different considerations found, along with their respective frequencies of mention, is presented in Table 2 below.

Table 2 - Procurement considerations found in the literature

	Article number																	
Consideration found in the literature	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*	*17*	*18*
Economic	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X	X
Physical/technical aspects	X				X	X	X					X	X	X	X	X	X	X
Ease of use	X				X							X						
Interoperability within hospital	X	X					X			X	X	X	X	X			X	
Post-market vigilance data		X			X													
Patient opinion		X		X		X												
Clinical data		X	X			X			X	X	X	X					X	X
End user preference			X			X		X	X				X	X	X	X	X	X
Sustainability					X							X						
Provider reputation and relation					X			X				X						
Patient outcome or experience					X	X	X		X	X	X			X				
Impact on local companies					X													
Delivery times								X										
Experiences of other doctors																		X

1.2.3 Identified knowledge gap

As detailed in section 1.2.2 and depicted in Table 2, numerous factors influence the procurement of medical devices and equipment. However, two notable knowledge gaps emerge from the literature. Firstly, only two studies included in this review discuss processes or policies in the Netherlands, specifically Brito Fernandes et al. (2022) and Blüher et al. (2019). This leaves a knowledge gap for mapping procurement practices and the involved actors within the Netherlands, given the potential differences in healthcare systems across countries. Secondly, none of the reviewed literature addresses the incorporation of cybersecurity in any capacity during the procurement process, while factors like cost-effectiveness and technical capabilities are commonly prioritised in device procurement. Yet, cybersecurity plays a crucial role in safeguarding hospitals against escalating cyber threat, as mentioned in the beginning of this introduction.

In summary, this thesis aims to address two key knowledge gaps: (1) by placing the research in the context of Dutch hospitals, it will contribute to better understand the procurement processes in the Dutch healthcare system and (2) this thesis will focus on cybersecurity and how it is, or can be involved in the procurement process, thereby trying to open the discussion on the significance of cybersecurity within Dutch hospitals. Additionally, it will explore stakeholders beyond hospitals, offering a broader perspective on the procurement process and its interrelations.

1.3 Research scope

As discussed earlier, this research will focus on the procurement process in hospitals of medical devices in the context of cybersecurity. For this, hospitals in the Netherlands will be approached and studied. This geographic boundary was chosen for three reasons. First, it will aid in filling in the first knowledge gap identified in the previous section. Second, as the researcher is based in the Netherlands it is easier to approach Dutch hospitals and language barriers are avoided. Finally, the focus on only one country allows for a more detailed analysis of the healthcare system, as this system may differ across countries. However, as most regulations are governed on an EU level, some of the results and recommendations of this thesis might still be applicable to other hospitals across the EU.

Second, this research will focus on the procurement of medical devices, as defined in section 1.1. This scope was chosen to reflect medical devices that in potential could be connected to the hospital's IT network, or even the internet. Because of this connection, cybersecurity could play a larger role than non-connected devices. Consequently, this research is scoped to these devices.

Finally, this study is scoped to include stakeholders from within the hospital and outside. A literature review from Hinrichs-Krapels et al. (2022) concluded that the procurement process of medical devices is an intricate process with various internal and external stakeholders involved. However, this literature review included only one study from the Netherlands, whilst department structures can differ per country and hospital. Therefore, the internal stakeholders identified by Hinrichs-Krapels et al. (2022) will guide the initial participant selection process. Yet, which stakeholders will exactly be interviewed is left open, as one of the goals of this thesis is to identify who contributes to the procurement process. Therefore, snowball sampling will be used to contact more stakeholders within a hospital.

In addition to internal stakeholders within the hospital, external stakeholders such as regulatory bodies and cybersecurity experts could also influence the procurement processes. These stakeholders might be actively engaged in the procurement process of new medical devices. For example, to request their expertise on cybersecurity matters. Therefore, it is important to also capture the perspectives of these stakeholders, given their indirect connection to the procurement process and their potential influence on hospitals to adopt specific policies.

1.4 Relevance

This research is relevant for both society and science. As discussed at the beginning of this introduction, societal relevance is supported in numerous ways. However, this research will mostly benefit society as it will provide recommendations on how the role of cybersecurity could be improved in the procurement process of new medical devices. This is beneficial for society as it will minimise risks such as identity theft and financial fraud (Coventry & Branley, 2018). Next to this, this research is also relevant for science in two ways. First, it will contribute to science by filling in the knowledge gaps found in section 1.2.3. Second, it will present new insights into the procurement processes in Dutch hospitals.

Next to societal and scientific relevance, this research is also relevant to the Complex Systems Engineering and Management (CoSEM) master's programme. More specifically the Information and Communication track which focusses on the governance and engineering of IT systems in complex (stakeholder) landscapes, as hospitals can be seen as intricate socio-technical systems in themselves (Jalali & Kaiser, 2018). Hospitals are vast organizations where a multitude of needs and interests from diverse stakeholders – such as patients, hospital staff, management, insurers, medical device manufacturers, and governments – must be considered. Moreover, even within these stakeholder groups, variations occur; for instance, various hospital departments may require different equipment and approaches to meet their specialized needs (Jalali & Kaiser, 2018). This complexity extends to the procurement process, which entails balancing the preferences of hospital staff and management with government procurement policies, manufacturer offerings and potential other stakeholders. Therefore, the chosen theoretical background in which this research is based also aligns with the CoSEM programme, as it will focus on the complexity of decision-making. Finally, previous research has called for a socio-technical view on cybersecurity in the healthcare domain (de Bruijn & Janssen, 2017; Williams et al., 2015), which also aligns with the CoSEM programme. Thus, this thesis will explore the alignment of different stakeholders on the hospital procurement processes in the context of cybersecurity, through a socio-technical lens.

1.5 Main research question and document structure

Following the previously discussed research gaps, scope, and relevance, the following main research question (MRQ) is used to guide this research:

To what extent are cybersecurity considerations integrated into the procurement process of medical devices in Dutch hospitals?

Chapter 2 will provide an overview of the research approach and methods, including an argumentation for the interviews and the accompanied analysis process. Following this chapter, the institutional environment surrounding procurement and cybersecurity within healthcare will be analysed. After, the results of the interviews will be discussed. The role of cybersecurity during the procurement process is discussed in Chapter 6. Hereafter, recommendations for hospitals are provided in chapter 7 Finally, a discussion and conclusion to this study will be provided in chapters 8 and 9.

2 Research approach and methods

This chapter will discuss the structured approach used to answer the MRQ. This is done by answering multiple sub questions (SQs), with various methods used to gather and analyse data to be able to answer the SQs.

2.1 Research approach

To determine what the current procurement practices of new medical devices are and how cybersecurity plays a role in this, a comparative case study approach is used, as suggested by Bryman (2016). The goal of such a comparative case study approach is to gain a deeper understanding of a social reality in different contexts. This method facilitates the comparison of multiple singular cases, where each case is examined individually and afterwards are compared. This will allow to pinpoint similarities and differences between the different cases. A case study approach based on interviews is chosen for this thesis to better grasp the social intricacies of the procurement process, instead of solely focussing on written processes and protocols set up by hospitals.

In addition, the comparative case study approach is essential for this thesis, as it is scoped to the Netherlands, and not just to one hospital. Therefore, different hospitals were approached to take part in this study. Each hospital is then treated as a single case study. Within a single case study, a case can be described as: “an object of interest in its own right, and the researcher aims to provide an in-depth examination of it” (Bryman, 2016, p. 61). This is applicable to this thesis, as each hospital’s approach to the procurement of medical devices and cybersecurity thereof will be examined on an individual basis. Afterwards, these different cases will be compared to identify differences and similarities between the hospitals’ approach to procurement and cybersecurity, therefore resulting in a comparative case study approach. By identifying these differences and similarities, a general view of the procurement process and cybersecurity aspects can be synthesised. Consequently, instead of focussing on a single case, or hospital, the comparative case study approach will allow for a better generalisation to the whole of the Netherlands.

2.2 Sub questions

To answer the MRQ and follow the research approach, five sub questions were synthesised to structure this research:

Sub question 1: How are cybersecurity considerations included in the current regulations and standards governing medical devices and the procurement thereof?

To establish a comprehensive view of the underlying framework of the procurement process and medical devices in general, an analysis of the current regulations and standards outlined by the Dutch Government, European Union, and other relevant regulatory bodies will be conducted. This analysis will serve as the initial reference point for assessing the alignment of various stakeholders with these regulations and evaluating their ability to support cybersecurity or integrate cybersecurity measures within the procurement processes.

Sub question 2: What are the existing general procurement practices for medical devices in hospitals in The Netherlands?

To be able to understand how cybersecurity is considered during the procurement process, the general procurement process per hospital needs to be mapped. Therefore, this sub question will focus on the general procurement practices, independent from cybersecurity. Additionally, the participating stakeholders and their views will be mapped. The various factors weighed by hospitals and stakeholders throughout the procurement process will be examined.

Sub question 3: What is the effect of external stakeholders on the procurement process of medical devices in the context of cybersecurity?

The procurement process in hospitals cannot be viewed as standalone and will be influenced by stakeholders from outside the hospital. These stakeholders can include, for example, regulatory bodies and cybersecurity experts. These actors might be actively involved in the process, such as cybersecurity experts, but could also shape the procurement process, such as regulatory bodies. However, other stakeholders could also include other doctors or hospitals that influence or are involved in the procurement process. Hence, this SQ will concentrate on the impact of external stakeholders on the procurement process.

Sub question 4: How are cybersecurity aspects considered compared to other considerations during the procurement of new medical devices?

The detailed procurement process mapped during sub question 2 will be used to derive a conclusion how cybersecurity aspects are considered during the procurement of medical devices. In addition, this will be compared to how other aspects are considered during the procurement process.

Sub question 5: What recommendations can be derived to improve the role of cybersecurity during the procurement process of new medical devices in Dutch hospitals, if at all?
As noted earlier, there is an increased societal relevance to enhance hospital cybersecurity. Therefore, this question will centre on providing hospitals ways to improve the integration of cybersecurity measures into the procurement process for new medical devices. This will be based on the findings of this study.

2.3 Research phases

This study will be divided into five phases, with each phase culminating in an artifact designed to contribute to answering the main research question. As previously stated, the objective of this research is to perform a comparative case study involving various stakeholders, resulting in an examination of the role of cybersecurity in the procurement of medical devices in the Netherlands. Data for this case study will be collected through desk research and stakeholder interviews. The research will take place in an iterative manner, allowing for newly gained insights in one phase to inform and refine previous phases or research artifacts. Below, the methodologies for each phase are outlined in detail.

Phase 1: Exploratory
During this first phase, the problem description, knowledge gap, scope, relevance, research questions, and theoretical background have been defined. To study and examine this, a structured literature review was done utilising Scopus. Scopus was selected as the research database due to its reputation as one of the most comprehensive sources of data across various fields (Pranckutė, 2021). Its inclusivity of diverse scientific disciplines enables a broader overview of the problem at hand compared to more specialised databases. Next to this, desk research was done to include non-scientific sources.
The insights gained from this general literature review and desk research have then been used to create the detailed research definition and theoretical background discussed in the preceding chapters.

Phase 2: Desk research
The second phase focussed on gaining a detailed overview of policies and scientific research on the topics of procurement in hospitals and cybersecurity. Specifically, it entailed a desk research and scientific literature review on sub questions 1, and 2. This will result in an overview of different policies related to procurement and cybersecurity. Additionally, scientific literature on the procurement process in Dutch hospitals will be used as a starting, and reference point for this study's mapping of the procurement process.

A literature review will be performed to study the current procurement processes in hospitals in the Netherlands, aligning with sub question two. This review will examine references to cybersecurity and the dynamics among various stakeholders involved during procurement processes and will be used as a starting and reference point for this study's mapping of the procurement process. Finally, desk research will take place to study the current cybersecurity and procurement regulations for hospitals in the Netherlands, in accordance with sub question 1. Policies or regulations that came up during the interviews of phase 3 will also be included in the policy overview. This background research will contextualise the procurement practices of hospitals within governmental and sectoral regulations and advice.

This phase results in a state-of-the-art overview of the current procurement practices in hospitals and the context in which it needs to operate.

Phase 3: Interview data gathering
This phase researched the different stakeholders involved in the procurement processes in hospitals. Drawing upon the state-of-the-art overview obtained during phase two, semi-structured interviews were conducted. Semi-structured interviews were chosen, as they allow for more spontaneous in-depth insights, whilst maintaining sufficient structure for a comparative analysis (Bryman, 2016). All interviews were held in Dutch, as to cater to the proficiency of the participants. This allows for a more fluent interview, which could result in different insights than when participants are asked to speak a language that they are not completely fluent in.

The interview population consisted of the stakeholders mentioned in sections 4.1 and 5.1. Therefore, representatives of external organisations knowledgeable on and involved in the procurement process in hospitals were interviewed, to research the view and influence of these organisations on the procurement process in the context of cybersecurity. For hospital stakeholders, different stakeholders involved with the process were contacted and interviewed. All roles that are involved with the procurement process within hospitals are considered. This will allow to map the procurement process within a hospital in a more detailed manner, whilst also mapping the interplay between different stakeholders. In total three hospitals are included, all of which non-academic. This resulted in a total of seven interviews conducted for this study.

Interviews are structured through the use of an interview protocol. Different protocols were used for internal stakeholders and external stakeholders. The interview protocol for internal stakeholders can be found in Appendix A.1, whilst the protocol for external stakeholders can be found in Appendix A.2. In these appendices both a Dutch version and an English translation is provided. As the interviews were conducted in Dutch, the Dutch protocol was followed. Furthermore, this study has been approved by the Human Research Ethics Committee (HREC) of the TU Delft under code 4028. This resulted in an informed consent form that participants were asked to sign prior to participation in this study. The informed consent form both in Dutch and English can be found in Appendix A.3.

All interviews were recorded and transcribed and form the basis for phase four. The information gathered in these interviews allow to answer sub questions one through four.

Phase 4: Interview analysis

To analyse the transcripts of the internal stakeholders, a framework analysis approach is used. The framework analysis method is a type of thematic analysis used to order and synthesise qualitative data (Bryman, 2016), in this case the interview transcripts. This method was chosen, as it allows for a structured way to compare different stakeholder groups (Bryman, 2016), therefore it is well suited to be used in the case of a comparative case study. Next to this, the approach is frequently used in the policy, healthcare, and nursing domains (Parkinson et al., 2016). A framework analysis consists of five different steps: (1) data familiarisation, (2) framework identification, (3) indexing, (4) charting, and (5) mapping and interpretation (Goldsmith, 2021). This phase will focus on creating the framework and will therefore focus on steps 1-4.

The first step provided an initial understanding of the interview transcripts and focussed on deriving major themes in the data. In the case of a larger dataset, as is the case here, this step only focusses on part of the data. This step also includes a preliminary set of codes linked to the data. The second step moved "the analysis from concrete descriptions of themes in the data to the identification of more abstract concepts, with the objective of providing a framework, or a structure for the analysis and the resulting interpretation" (Goldsmith, 2021, p. 2065). Such a framework usually contains major themes, supported by several sub-themes. This step also included some coding, as the initial codes were refined, and some new codes were added to support the sub-themes. The next step focussed on applying the created framework to the whole dataset and required the whole dataset to be coded. The data was indexed based on the different stakeholder types and individual stakeholders. As the framework was now applied to the whole dataset, small revisions were made to the framework during this step. The goal of the fourth step is to order and abstract the indexed data in one or more charts in a matrix form. This provided an initial understanding of the procurement process and allows for comparisons to be made.

As can be concluded from the paragraph above, a framework analysis is an iterative process, where refinements are made in each step. Therefore, coding was done in ATLAS.ti, a qualitative analysis software tool. This allows for easier manipulation of the coding throughout the whole process and to keep track of the framework being created.

In contrast to the internal stakeholders, only one external stakeholder was interviewed. Therefore, a framework analysis is not suited, as there is no comparison to be made. Consequently, for the external stakeholder interview a thematic analysis was performed. A thematic analysis is comparable to the first two steps of the framework analysis, (1) data familiarisation, and (2) framework identification. Coding was also done in ATLAS.ti.

Phase 5: Synthesis

In the synthesis phase, insights gained from the literature review, desk research, and framework analysis are combined in a comparative case study. This facilitates an examination of each case individually and in relation to one another (Crowe et al., 2011). This analysis is supported by a theoretical background that serves as an academic lens to look at the innerworkings of the procurement process. The outcome is a detailed overview of the complete procurement process within Dutch hospitals in the context of cybersecurity. Furthermore, an evaluation of the alignment of the various stakeholders involved in the process on the importance of cybersecurity in procuring new medical devices is provided. Utilising the mapping and interpretation of the framework analysis, a conclusion is drawn to address the main research question. Finally, recommendations drawn from the results will be detailed to help hospitals balance the cybersecurity aspect with other aspects in their procurement process.

2.4 Research flow diagram

To visualise the research flow, a diagram outlining the research flow is presented in Figure 3 below. This diagram details each step of the research process along with its corresponding sub question. Whenever specific research methods are used to advance to the following research step, they are indicated within the arrows. Additionally, intermediary research outcomes are represented by file icons.

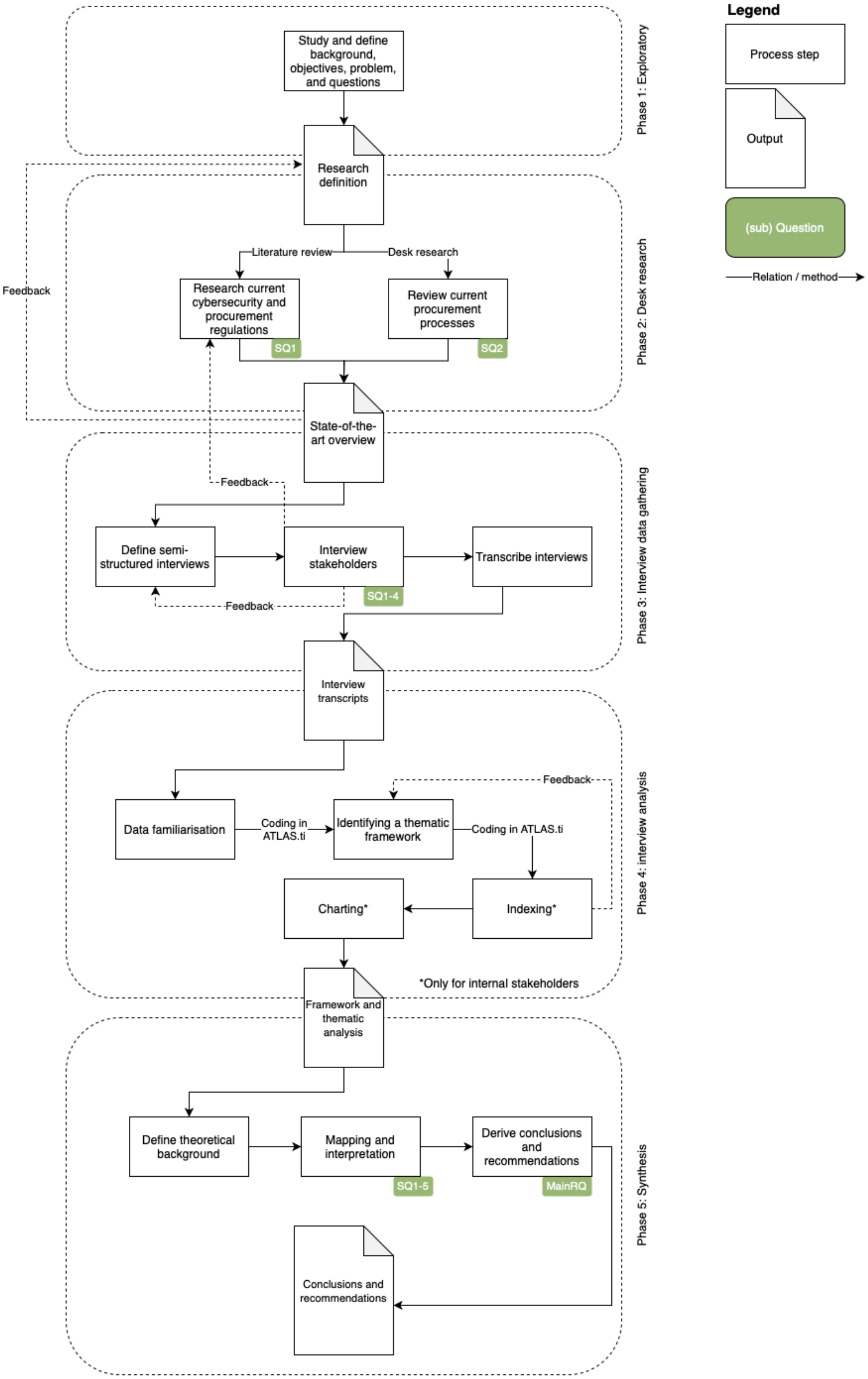

Legend
Process step
Output
(sub) Question
Relation / method
Phase 1: Exploratory
Study and define background, objectives, problem, and questions
Research definition
Phase 2: Desk research
Literature review
Desk research
Feedback
Research current cybersecurity and procurement regulations
SQ1
Review current procurement processes
SQ2
State-of-the-art overview
Phase 3: Interview data gathering
Feedback
Define semi-structured interviews
Interview stakeholders
SQ1-4
Transcribe interviews
Feedback
Interview transcripts
Phase 4: interview analysis
Data familiarisation
Coding in ATLAS.ti
Identifying a thematic framework
Feedback
Coding in ATLAS.ti
Charting*
Indexing*
*Only for internal stakeholders
Framework and thematic analysis
Phase 5: Synthesis
Define theoretical background
Mapping and interpretation
SQ1-5
Derive conclusions and recommendations
MainRQ
Conclusions and recommendations

Figure 3 - Research flow diagram

3 Institutional Environment

This chapter will focus on the policy context in which manufacturers, hospitals, service providers, retailers, etc. need to operate when it comes to cybersecurity for medical devices. An emphasis will be put on manufacturers and hospitals, as these stakeholders align with this study. This will provide the policy background for this thesis and will answer SQ1: *How are cybersecurity considerations included in the current regulations and standards governing medical devices and the procurement thereof?*

As this study focusses on The Netherlands, the policies set out by the European Union (EU) will be detailed below. However, as manufactures often work on an international scale, it is important to also include international policies (MDCG, 2020). Therefore, this chapter will also detail the policies set out by The United States, as it is the biggest market for medical devices (MedTech Europe, 2023).

3.1 European Union

Within the EU, three main policies for medical device cybersecurity are considered: the Medical Devices Regulation, the Network and Information Systems Directive, and the General Data Protection Regulation. These three policies are detailed below.

3.1.1 Medical Devices Regulation

In 2017 the EU adopted the Medical Devices Regulation (MDR), which reached full implementation in 2021 (Ludvigsen, 2023). This regulation, known under the code (EU) 2017/745, replaced the previous Medical Devices Directive (MDD) with the goal of ensuring that medical devices are, amongst others, better fit for new technological challenges (MDCG, 2020). Although the MDR is very broad, this section will solely focus on its implications on cybersecurity.

While the MDR lacks explicit directives on cybersecurity, integrating cybersecurity protocols in medical devices is imperative to adhere to the general requirements set out by the MDR (Ludvigsen, 2023). The main requirements depicted by the MDR include various risk management systems, financial management, and quality assurance for medical devices (Regulation (EU) 2017/745, 2023), where cybersecurity cannot be neglected. Next to this, the MDR includes the general notion that medical devices should be able to continue to operate when they face any malicious attack (Ludvigsen, 2023). To help manufacturers interpret the underlying cybersecurity directives in the MDR, the Medical Device Coordination Group (MDCG) released a report with guidance on the topic (MDCG, 2020). The MDCG was established by the European Commission at the same time as when the MDR was implemented in 2017, with the goal, amongst others, to develop guidance “aimed at ensuring effective and harmonised implementation” of the MDR (Regulation (EU) 2017/745, 2023). Therefore, their report on cybersecurity for medical devices is used to detail the cybersecurity requirements set out by the MDR.

The cybersecurity requirements set out in Annex I of the MDR can be divided in pre- and post-market directives (MDCG, 2020). Key for all directives is that manufacturers must consider the state-of-the-art within their decision-making process. This can be based on sector standards, guidance documents such as the one of the MDCG, proprietary manufacturer knowledge, or publicly available (scientific) knowledge. Given the notion that manufacturers must consider the state-of-the-art, effectively means that Member States of the EU can require a medical device’s cybersecurity to be state-of-the-art as well. Table 3 depicts all activities manufacturers must follow to comply with the cybersecurity requirements set out by the MDR.

Table 3 - Cybersecurity activities required by the MDR, adapted from MDCG (2020)

Pre-market activities	*Post-market activities*
Adhere to secure by design	
Risk management	Risk management
Establish risk control measures	Modify risk control measures / corrective actions / patches
Perform validation, verification, risk assessment, benefit risk analysis	Perform validation, verification, risk assessment, benefit risk analysis
Provide technical documentation	Maintain and update a post-market surveillance plan and post-market surveillance system
Perform conformity assessment	Trend reporting

Pre-market activities	*Post-market activities*
Establish a post-market surveillance plan and post-market surveillance system	Analysis of serious incidents
Publish clinical evaluation process	Publish post-market surveillance report
	Publish periodic safety update report
	Update technical documentation
	Inform the electronic system on vigilance

As can be seen in Table 3 above, a lot of the requirements revolve around administrative measures and mitigating current and future risk. This is done through the obligation of providing documentation on the medical devices and by performing continuous assessments and analyses. However, when it comes to implementing cybersecurity measures into the medical device itself, the principle of secure by design is most important. This principle leads to a so-called defence-in-depth strategy for medical devices. To come to this strategy, MDCG (2020) identified eight different practices manufacturers should follow:

> *Practice 1: Security management*
> The aim of the first practice, security management, is to make certain that security-related tasks are planned, documented, and carried out across the product's lifespan. This practice should also be applied during all other practices as to ensure that all practices are documented and carried out. (MDCG, 2020)
>
> *Practice 2: Specification of security requirements*
> The procedures outlined in this practice are employed to determine the necessary security features for safeguarding the confidentiality, integrity, and availability (CIA) of services, data, and functions provided by the device, considering the specific security requirements of the device. These security features may comprise authentication, authorisation, encryption, auditing, and other measures. Additionally, the product's security context includes factors such as physical security measures and safeguarding external interfaces through firewall protection, among others. (MDCG, 2020)
>
> *Practice 3: Secure by design*
> The procedures outlined in this practice are employed to guarantee that the product is secure by design, leading to the principle of defence in depth. (MDCG, 2020)
>
> *Practice 4: Secure implementation*
> This practice focusses on that the product functionalities are implemented in a secure manner. Requirements set out in this practice apply to all elements related to software and hardware within the product, excluding externally sourced elements. For such externally sourced elements, practice 1 should be followed. (MDCG, 2020)
>
> *Practice 5: Security verification and validation testing*
> The procedures outlined in this practice are used to record the security evaluation necessary to verify compliance with all security requirements for the product, ensuring the product's security during its intended use. Security testing should be coordinated with other product testing activities and may be performed at different stages by different individuals throughout the entirety of the security lifecycle, based upon the testing type and the manufacturer's chosen development model. (MDCG, 2020)
>
> *Practice 6: Management of security-related issues*
> This practice details processes that can be utilised to deal with security-related issues of a medical device. (MDCG, 2020)
>
> *Practice 7: Security update management*
> The procedures outlined in this practice are employed to guarantee that security updates and patches related to the product undergo testing to identify any potential setbacks and are promptly distributed to product users. (MDCG, 2020)
>
> *Practice 8: Security guidelines*
> This practice depicts procedures that are employed to provide and maintain user documentation detailing the integration, configuration, and maintenance procedures necessary to implement the defence-in-depth strategy of the medical device in alignment with its specific security context. (MDCG, 2020)

The way these practices and the defence-in-depth strategy for medical devices relate to each other is depicted in Figure 4 below.

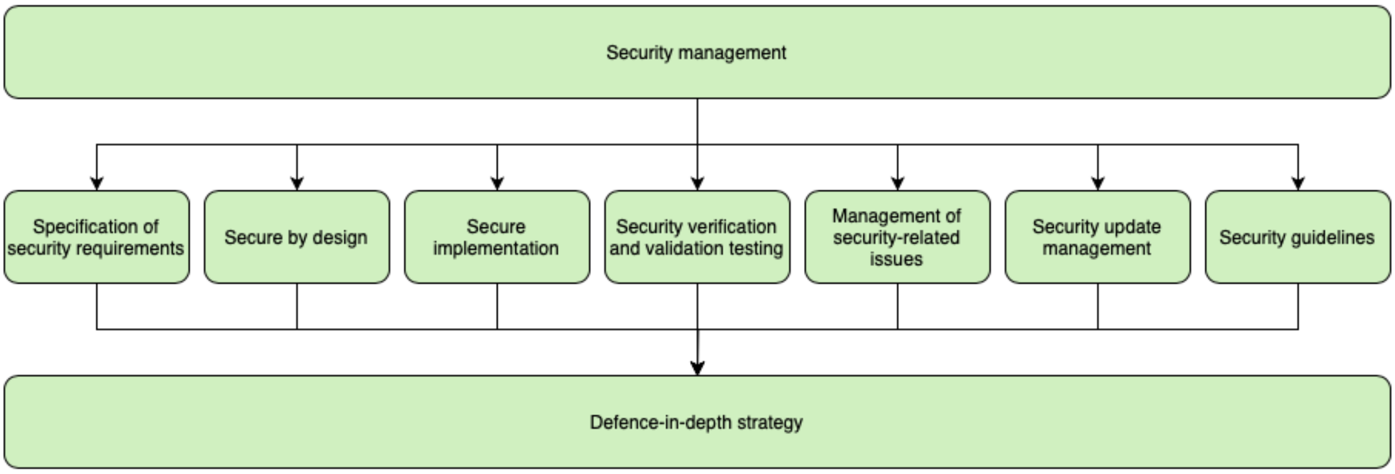

Security management
Specification of security requirements
Secure by design
Secure implementation
Security verification and validation testing
Management of security-related issues
Security update management
Security guidelines
Defence-in-depth strategy

Figure 4 - Defence-in-depth strategy, adapted from MDCG (2020)

However, besides directives that manufactures should follow, the MDR also details requirements for the integrator, operator, and user of the medical device (MDCG, 2020). The integrator and operator can be the hospital itself, or a third-party. The integrator is tasked with the installation and configuration of the medical device and the integration into the environment of the operator. It is crucial for the integrator to ensure that the system is configured to operate securely within the targeted environment. Integration itself should not modify or expand the intended use of the medical functions of the devices. However, it does create the opportunity to enhance information security, as it allows for the implementation of additional protection measures related to the specific integration environment, i.e. encryption or user roles. Yet, the responsibility for ensuring the information security of an integrated medical device remains with the hospital if it has tasked the integrator with connecting the device to the hospital's IT network.

The operator is tasked with the maintenance and facilitates the daily use of medical devices. Therefore, it bears the responsibility for procurement, and must guarantee the maintenance of security throughout the operation of the medical device, ensuring that it is not jeopardised by changes in the environment or by user interaction. The operator can adhere to this responsibility by following the requirements and guidelines for security detailed by the manufacturer. For example, these requirements and guidelines can be to isolate the device from the internet when this is not needed for its operation and to ensure that all software updates are installed as instructed by the manufacturer.

Finally, the user of the medical device (e.g. doctors, nurses, radiologists) must only use the medical device for its intended purpose. Next to this, they should use the device in a cybersecure manner, such as using strong passwords and being aware of potential cyber risks.

In conclusion, the implementation of the MDR, particularly concerning cybersecurity, has slightly impacted the procurement of medical devices, as the focus mainly lies on device security itself. While the MDR lacks explicit directives on cybersecurity, its broad requirements necessitate the integration of cybersecurity protocols to ensure compliance. Manufacturers must adhere to cybersecurity measures outlined in Annex I of the MDR, focusing on both pre- and post-market activities to mitigate current and future risks effectively. Additionally, responsibilities extend beyond manufacturers to integrators, operators, and users, emphasising the importance of maintaining security throughout the device's lifecycle. Integrators must ensure secure installation and configuration, while operators bear the responsibility for maintenance and daily operation, guided by the manufacturer's security requirements. Here procurement does play a role, as the medical device must be able to be securely integrated into a hospital's network and be compatible with the network's security standards. Ultimately, users must utilise devices only as intended and in a cyber secure manner, emphasising the collaborative effort required to safeguard medical device cybersecurity under the MDR.

All specific requirements related to the cybersecurity of medical devices set out by the MDR are detailed in Appendix B.

3.1.2 Network and Information Security Directive

The Network and Information Security 2 Directive (NIS2), otherwise known as Directive (EU) 2022/2555, replaces the previous Network and Information Security (NIS) directive per October 2024. It is important to consider the NIS2, as it directly relates to medical device and hospital cybersecurity (Ludvigsen, 2023; MDCG, 2020). The original NIS directive was implemented in 2016 with the goal to impose a common level of cybersecurity for essential digital services and other digital services operators across the EU (Vandezande, 2024). However, being a directive, it requires Member States to incorporate it into their national legislation rather than being universally applicable across the EU like a regulation is. Consequently, this process has led to varying laws among Member States, primarily because different countries have employed a variety of methods for identifying essential services (Biasin & Kamenjašević, 2022; Singh, 2023; Vandezande, 2024). Therefore, the NIS2 entered into force on January 16th, 2023, in an effort to harmonise the legislation across Member States by further defining requirements and affected organisations (Biasin & Kamenjašević, 2022; Singh, 2023). The new directive must be transposed by Member States before Ocotber 18th 2024 (Singh, 2023). Consequently, the precise impact of the directive remains uncertain (Singh, 2023), and the Dutch government has yet to release their transposition of the directive. Therefore, this section will focus on the changes made with the NIS2 directive and the preliminary guidance documents the Dutch government has already released. Consequently, this section will discuss the registration and reporting obligations, minimum cybersecurity requirements, management body responsibility, and the supervision by Member States.

As mentioned earlier, one of the main problems which NIS2 tries to fix is the divergence per member state of organisation considered by the directive. Consequently, some hospitals were marked as essential entities by one Member State, whilst another Member States did not (Vandezande, 2024). Therefore, NIS2 expands and better defines its list of entities considered 'essential' and adds entities it considers 'important' (Singh, 2023). This elaboration of the list results in hospitals always considered essential and medical device manufacturers considered either essential or important, based on the importance of the devices they manufacture and the size of the company (Biasin & Kamenjašević, 2022; Ministry of Economic Affairs and Climate Policy, n.d.-b; Singh, 2023). The entities considered important or essential are obliged to register themselves at the respective national cybersecurity agency of the Member State they are situated in (Directive (EU) 2022/2555, 2022), in the Netherlands this will be the Nationaal Cyber Security Centrum (NCSC) (Ministry of Economic Affairs and Climate Policy, n.d.-a).

Cybersecurity policies often fail because IT departments in organisation often don't get the appropriate recognition and corresponding funding and support from upper management (Vandezande, 2024). Therefore, the NIS2 directive puts greater responsibility on 'management bodies' of entities to ensure compliance with the directive (Singh, 2023; Vandezande, 2024). It is up to the Member States to define what a management body is, which means that it remains unclear who is directly affected by this new policy until the directive is transposed into law (Singh, 2023). However, it introduces four new policies which affects management bodies (Singh, 2023):

1. Management bodies should sign off on all cybersecurity risk management measures to be implemented by the entity to ensure compliance with the NIS2 directive.
2. Management bodies should follow regular cybersecurity trainings to be able to understand, assess, and manage the cybersecurity risks posed to the entity.
3. Management bodies supervise the integration of selected cybersecurity risk management measures within the entity.
4. Management bodies are liable in the case of non-compliance with the NIS2 directive.

Article 21 of the NIS2 imposes 10 minimum cybersecurity requirements in the form of "cybersecurity risk-management measures" (Directive (EU) 2022/2555, 2022), in Dutch called "zorgplichtmaatregelen" (Ministry of Economic Affairs and Climate Policy, n.d.-a). Although the exact requirements need to be set by each Member State and therefore remain unclear (Singh, 2023), the general requirements are as follows (Directive (EU) 2022/2555, 2022; Ministry of Economic Affairs and Climate Policy, n.d.-a):

1. **Policies on risk analysis and information system security:** an entity must perform a risk analysis on the organisation which identifies the major risks and potential security measures needed to avoid these risks.
2. **Incident handling:** to be able to respond to an incident in an adequate manner, an Incident Response Plan (IRP) should be in place. An IRP includes a set of actions organisations should follow when an incident occurs. How an IRP exactly looks like differs per organisation, but can include for example different scenario's, who is responsible for what in case of an incident and how you will recover from an incident.

3. **Business continuity:** a plan should be in place to guarantee business continuity in case of unexpected events, such as a cyber-attack. Such a plan can build upon the IRP but should include measures to maintain business operations such as backup management, disaster recovery (how to fall back on other systems), and redundancy.
4. **Supply chain security:** an entity should assess the cybersecurity level of its direct suppliers and service providers. This measure is closely related to procurement, as this assessment should also be part of the selection procedure of new suppliers or providers. An entity should also make clear how they intent to deal with the risk imposed by the supplier or provider they choose. Therefore, this implies that suppliers should be able to demonstrate a certain level of cybersecurity, even though they are not directly impacted by the NIS2 directive. Consequently, the new NIS2 directive has to potential to influence way more entities than that are directly impacted by the directive (Vandezande, 2024).
5. **Security in network and information systems acquisition, development, and maintenance:** policies should be in place that manage the security of network and information systems in terms of acquisition, development, and maintenance. Examples of such policies include change management, patch management, vulnerability management, and procurement policies.
6. **Policies and procedures to assess the effectiveness of cybersecurity risk-management measures:** after a risk analysis has been performed and suitable security measures have been put into place, the effectiveness of these measures should be evaluated. How this is evaluated is up to the organisation.
7. **Cybersecurity training and basic cyber hygiene:** an entity should follow basic cyber hygiene rules such as the ones set out by the NCSC. Furthermore, employees should be made aware of cybersecurity risks by following a cybersecurity training.
8. **Policies and procedures regarding the use of cryptography and encryption:** an entity should have appropriate policies and procedures in place that describe the techniques used to ensure the confidentiality and integrity of information systems. These policies should be revised periodically to ensure effectiveness.
9. **Human resource security, access control, and asset management:** human resource security is related to measure 7, but also includes screening of the employees on reliability. Access control depicts who has access to which system and what data and for how long they have access for. Here it is best practice to follow the principle of least privilege, meaning that users have as little access as possible. Finally, asset management requires entities to map all hard- and software managed by the organisation and all devices connected to the IT infrastructure. Then, all assets should be assessed based on the Confidentiality, Integrity, and Availability (CIA) principle and should be maintained accordingly.
10. **The use of multi-factor authentication, secured voice, video, and text communications, and secured emergency communication systems:** this measure imposes the use of multi-factor authentication when logging into systems. This means that besides a password, a user should also either use some sort of biometric authentication or a security key/code to log in. For secured communications, an organisation can use a Virtual Private Network (VPN) to secure all communication between devices, independent of the network they are on.

Third, entities have the obligation to report any significant incident that occurs to the Computer Security Incident Response Team (CSIRT) (Ministry of Economic Affairs and Climate Policy, n.d.-a). The NIS2 directive defines a significant incident in Article 4 (5) as follows: “any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the related services offered by, or accessible via, network and information systems” (Directive (EU) 2022/2555, 2022). If this is the case, entities should make three reports (Singh, 2023; Vandezande, 2024):

1. Within 24 hours of the incident, an initial warning should be given.
2. Within 72 hours of the incident, an incident notification should be reported with an initial assessment of the impact and severity, and any indicators of compromise.
3. Within 1 month of the incident, a full report should be submitted with the full details of the incident and its cause.

If the incident involves personal data, then it will most likely also fall under the GDPR discussed in the next section, which means that the relevant national data authority should also be notified (Singh, 2023).

Finally, all NIS2 entities will be supervised to ensure compliance by a national supervisor (Biasin & Kamenjašević, 2022). This supervisor will proactively supervise essential entities, whilst important entities can only be investigated when an incident has occurred (Singh, 2023). Investigations can include security audits and inspections, security scans, request for cybersecurity measures, and more (Singh, 2023). In the Netherlands, the organisation tasked with this supervision has yet to be determined (Ministry of Economic Affairs and Climate Policy, n.d.-a).

In conclusion, NIS2 impacts the procurement of medical devices by emphasising a more holistic approach to cybersecurity governance. By extending and refining the categorisation of essential entities, including hospitals and medical device manufacturers, NIS2 mandates rigorous registration and compliance measures. Moreover, the directive places heightened responsibility on management bodies to oversee cybersecurity risk management, training, and implementation, underscoring the imperative for organisational commitment to cybersecurity. Importantly, NIS2 introduces more stringent minimum cybersecurity requirements, impacting procurement processes by necessitating an assessment of supply chain security and adherence to security protocols. Therefore, an extra step is introduced in the procurement process where hospitals will have to ask their suppliers which cyber reassurances they can give. Additionally, incident reporting obligations and supervisory mechanisms ensure accountability and compliance, which could further influence procurement decisions and practices.

3.1.3 General Data Protection Regulation

The General Data Protection Regulation (GDPR) replaced the Data Protection Directive of 1995 in an effort to harmonise data laws of the different Member States of the EU. The regulation, known under the code (EU) 2016/679, came into effect in May 2018. As the regulation covers the way that data is processed and stored, it is important to also consider the cybersecurity aspects of this regulation (European Union Agency for Cybersecurity et al., 2020). Next to this, the GDPR complements the MDR in the aspects of cybersecurity and liabilities (Yeng et al., 2020). Therefore, this chapter will first outline the general notion of the regulation, thereafter its application to the healthcare domain will be discussed. Finally, the implications for cybersecurity will be detailed.

GDPR in general

The GDPR's sole focus is on natural persons and their personal data (Council of Europe et al., 2018). The regulation identifies a natural person in article 4(1) as someone "who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (Regulation (EU) 2016/679). Examples of such personal data include contact details, work details, fingerprints, IP addresses, etc. Besides the basic personal data, the GDPR makes a distinction between special personal data and sensitive personal data. The latter is data that has a larger impact on the privacy of a natural person than basic personal data such as name or a phone number and therefore must be protected better. Examples of sensitive personal data include salary, location data, and bank statements (Council of Europe et al., 2018). Special personal data is data that reveals "racial or ethnic origin, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation" (Regulation (EU) 2016/679). Processing such data is prohibited, unless one of the exceptions in Article 9(2) of the GDPR applies. One of these exceptions is for hospitals, which allows them to process health data.

In the previous paragraph, the processing of data was mentioned several times. Under the GDPR processing relates to any operation performed on personal data, either automatic or manually (Council of Europe et al., 2018). Processing can be done by for example collecting, recording, organising, using, adapting, or retrieving personal data (Regulation (EU) 2016/679). Concrete examples of this include using an email address to send an email or offering an online contact form.

The legal responsibility for the GDPR is shared between the so-called controller and processor (Council of Europe et al., 2018). The controller can be a natural or legal person or public authority who determines the purpose and means of processing. In this case, this will most often be the hospital itself. The processor can also be a natural or legal person or public authority but is tasked with processing the data on behalf of the controller, following the controller's instructions. In the case of this thesis, this can be the hospital itself, but also third parties that process the data on behalf of the hospital. For example, a processor can be a cloud-based data storage provider which the hospital uses to store their data (Council of Europe et al., 2018). The main legal liability remains with the controller, as this entity determines why and how data is processed. However, both must comply with the regulations set out by the GDPR. These regulations can be summarised into the seven key principles of the GDPR (Council of Europe et al., 2018):

> *Principle 1: Lawfulness, fairness, and transparency of processing*
>
> The GDPR requires that personal data must be processed in a lawful manner. Lawful processing requires either the consent of the natural person or another legitimate ground. A legitimate ground can be when the processing is necessary for the performance of a contract, when there is a legal obligation, if it is necessary to protect the vital interests if a natural person, when it is needed for the public interest or for the purpose for the controller's legitimate interest. Fairness depicts that the controller must be able to demonstrate their compliance with the GDPR. Next to this, processing may not be done in secret and natural persons should be notified of the potential risks. Finally, transparency requires the controller to notify the natural person that there is being processed,

should be able to communicate this in clear and understandable language, and gives natural persons the ability to access their data. (Council of Europe et al., 2018)

Principle 2: Purpose limitation
Personal data may only be processed for one or more specified purposes defined at the beginning of the processing. This means that prior to collection, it must be clear for what specific, explicit, and legitimate purposes the data will be processed. After initial collection, the data may not be used for other purposes that are incompatible with the original purposes. If it is desired to undertake additional processing, the natural person should be informed of the new purposes and have the right to object. (Council of Europe et al., 2018)

Principle 3: Data minimisation
The processing of personal data should be limited to what is necessary to fulfil the purpose. This means that the controller should only collect data that is directly relevant for the specific purpose of the processing. Next to this, when privacy-enhancing technology can be used to avoid the collection of personal data entirely, then that should be utilised by the controller. (Council of Europe et al., 2018)

Principle 4: Data accuracy
Personal data may only be processed when the controller is sure that the data is accurate and up to date. Therefore, all reasonable steps should be taken to delete or correct inaccurate data in a swift manner and on a regular basis. In some cases, updating data is prohibited, as the principal purpose of storing the data was to document certain historic events. An example of this can be a medical record of an operation that was performed that includes findings that are later deemed wrong. In that case only additions to the data may be made. (Council of Europe et al., 2018)

Principle 5: Storage limitation
The processing of personal data needs to stop after the purpose for which it was collected has been fulfilled. Consequently, the data will need to be deleted, returned, or anonymised after processing. Exceptions on this principle apply when the data is anonymous, or if data is archived for public interest, scientific or historical purposes. (Council of Europe et al., 2018)

Principle 6: Data security
This principle is most related to cybersecurity, as it is concerned with the security and confidentiality of personal data. The goal of this principle is to protect the data subject from harm caused by unlawful processing of their data but also the lost or theft of data. Therefore, the controller and processor must consider the state-of-the-art when implementing technical or organisational security measures. A technical measure can be for example having proper cybersecurity in place, whilst an organisational measure can be to have strict access rights to the data. The GDPR also advices to pseudonymise the data to minimise the adverse effects when data is stolen. (Council of Europe et al., 2018)

Principle 7: Accountability
Accountability requires controllers and processors to comply with the elements of the GDPR. The principle also requires them to be able to demonstrate their compliance to data subjects, the general public or authorities. It also holds controllers accountable for their duty to protect the data they have collected through technical and organisational measures. Finally, controllers should also see to it that all other parties involved in processing the data, such as the processor or sub-processors, comply with the GDPR. (Council of Europe et al., 2018)

GDPR for hospitals

All aforementioned of course also apply to hospitals. However, as mentioned in the previous section, medical data is considered special personal data under the GDPR. This means that hospitals have the exception to be able to process this kind of data (Regulation (EU) 2016/679). Next to this, hospitals may store data longer than initially planned when they use it for research purposes. In that case, the data needs to be anonymised or pseudonymised (Council of Europe et al., 2018).

However, processing special personal data may result in a high risk to the freedom and rights of a natural person. Therefore, hospitals are required, as controllers, to conduct a data protection impact assessment (DPIA) before processing begins (Regulation (EU) 2016/679). In the DPIA, controllers should evaluate the origin, nature, and severity of potential risks to the natural person. Hereafter, suitable measures should be taken into account to safeguard the natural person. DPIAs should be updated continuously rather than be conducted one time, even after the start of processing.

There is no set format for a DPIA, but it should at least consider "the nature, scope, context and purposes of the processing and the sources of the risk […] the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance [with the GDPR]" (Regulation (EU) 2016/679). Finally, in the case of a data breach, hospitals are obliged to report according to the NIS2 directive (European Union Agency for Cybersecurity et al., 2020).

GDPR and cybersecurity

The cybersecurity implications of the GDPR are relatively limited, as it is only concerned with protecting personal data (Ludvigsen, 2023). However, to comply with the data security principle, hospitals should consider the state-of-the-art in technical and organisational measures to safeguard data. In the case of technical measures, this means that hospitals should consider the state-of-the-art in terms of cybersecurity. However, they are not obliged to implement the state-of-the-art, as the costs should weigh up to the benefits (Council of Europe et al., 2018). Next to this, the GDPR is not clear on what the state-of-the-art is or how this can be determined. Therefore, the exact implications of the GDPR on cybersecurity remains uncertain.

In the Netherlands, in addition to the GDPR the NEN7510 norm exists which makes certain principles of the GDPR more concrete (NEN, 2017). Although it is not mandatory for hospitals to follow this norm, it is deemed good practice to do so (Ludvigsen, 2023). The NEN7510 norm focusses on information security in the healthcare sector and discusses several practices hospitals should follow to adequately handle health data through a controlled process. The goal is to ensure that health data is always available and that the integrity and confidentiality of the data is guaranteed. This is important, as health data should remain personal and should not suddenly become unavailable to a healthcare professional due to an update of the IT systems (NEN, 2017). Examples of these practices include how the hospital should be organised, staff screening, access rights, physical security of systems, cryptographic measures, procurement, incident reporting, etc (NEN, 2017). If they implement all practices depicted by the NEN7510 norm, they will automatically also comply with the GDPR, which emphasises that the NEN7510 norm is an addition to the GDPR.

In conclusion, the GDPR slightly affects the procurement of medical devices. The GDPR's focus is on safeguarding personal data, including sensitive medical information. Hospitals, as controllers of this special personal data, are obligated to adhere to the GDPR's principles, ensuring lawful, fair, and transparent processing, as well as robust data security measures. Specifically, the GDPR mandates that hospitals conduct DPIAs to evaluate and mitigate risks associated with processing sensitive data. This is where the GDPR could influence the procurement of new medical devices the most, as hospitals might base their decision on this assessment and manufacturers should be able to comply with this assessment. Furthermore, in the Netherlands, adherence to the NEN7510 norm supplements GDPR compliance, offering a more concrete framework for information security practices within the healthcare sector. How this affects procurement is discussed in section 3.4.1.

3.2 United States

As medical device manufacturers often operate on an international scale, they are affected by policies from different countries. Therefore, both Ludvigsen (2023) and the European Union Agency for Cybersecurity (ENISA) (2020) identified policies of the United States (US) as relevant to consider based on the size of the US market for medical devices. Although these policies do not directly influence hospitals and their procurement of medical devices, it still can influence the cybersecurity policies of manufacturers. Consequently, this section will briefly discuss the different policies set out by the Food and Drug Administration (FDA) and the Health Insurance Portability and Accountability Act (HIPAA).

3.2.1 Food and Drug Administration

In the US medical devices are governed federally by section 201(h) of the Food, Drug, and Cosmetics Act, and the federal regulatory body the Food and Drug Administration (FDA) (Food, Drug, and Cosmetics Act, 2018). The FDA has the power to classify what medical devices are and assess their compliance with their regulations (Ludvigsen, 2023). It does this based on an *ex-ante* evaluation, which means that medical devices are evaluated prior to their admission to the market and, contrary to the EU, are generally not supervised once they are approved (Ludvigsen, 2023). Medical Devices may be approved at the discretion of the FDA, showcasing its extensive authority in decision-making. This displays a significant contrast between the United States and the European Union in the regulation of medical devices (Ludvigsen, 2023).

Some acts do exist for cybersecurity that manufactures have to comply with. These acts include sections 3060 and 3060(a) of the 21st Century Cures Act and the Policy for Device Software Functions and Mobile Medical Applications, mandating sufficient cybersecurity measures to ensure the proper operation of medical devices, which introduces a need for more detailed cybersecurity considerations (Ludvigsen, 2023). Yet, the PATCH Act of 2022 has proven to be more influential. The act introduces the legal authority and obligation for the FDA to take cybersecurity into account when approving medical devices (Khalil, 2023). It requires manufacturers to release cybersecurity updates for vulnerabilities during the whole lifecycle of the medical device, to maintain a high level of cybersecurity throughout the use of the device (PATCH Act of 2022), including a plan to monitor, identify, and address these vulnerabilities (FDA, 2024). Second, it requires manufacturers to provide a software bill of materials, that details all soft- and hardware that is included in the medical device (FDA, 2024). Third, manufacturers should have the appropriate cybersecurity measures in place to ensure secure operations of the device and related systems (FDA, 2024). However, Ludvigsen (2023) points out that due to the ex-ante evaluation and the absence of ex-post inspections, compliance throughout the device's lifecycle is not ensured, which could lead to an increased cybersecurity vulnerability of the device.

Next to these acts, the FDA issued two guidance documents on cybersecurity for medical devices in 2016 and 2023, to guide manufacturers in the right direction for approval. These guidance documents identify cybersecurity issues that should be addressed by the manufacturer (Schwartz et al., 2018).

The 2016 guidance document "Postmarket Management of Cybersecurity in Medical Devices" promotes the implementation of a proactive, comprehensive cybersecurity risk management approach after the device has been approved. Such an approach can be integrated into the risk management process and may involve various measures, including (FDA et al., 2016; Lechner, 2017):

1. Monitoring cybersecurity information sources such as the CVE (Common Vulnerabilities and Exposures) standard for information security vulnerabilities.
2. Establishing software lifecycle processes.
3. Assessing and identifying the presence and impact of vulnerabilities.
4. Defining communication processes for vulnerability intake handling.
5. Regularly utilise a threat model.
6. Establish a policy on how to disclose vulnerabilities.
7. Deploying mitigations for identified cybersecurity risks early and before they are exploited.

The 2023 guidance document "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions" focusses on the premarket submission and supersedes a document from 2014 on cybersecurity in medical devices. The guidance document focusses on ensuring that medical devices are designed securely so that they are more capable of mitigating cybersecurity risks throughout the device's lifecycle. It adheres to the principles of secure by design and transparency, meaning that manufactures take cybersecurity into account from the beginning and are transparent about the risks that remain. To identify and mitigate potential risks during the development of medical devices, the FDA promotes the use of the Secure Product Development Framework (SPDF). After the device has been developed, manufacturers should include a security risk management in their submission, which entails: a threat model, a cybersecurity risk assessment, interoperability considerations, included third-party components and software, security assessment of unresolved anomalies, and lifecycle security risk management. Besides the cybersecurity of the device itself, the manufacturer should also consider the environment in which it will operate. Here, again, risks should be identified and mitigative measures should be implemented, such as measures for authentication, cryptography, or event logging. Finally, all measures implemented should be tested to prove efficacy. To make sure that the device is used in a correct manner by the end user, transparency is essential. Therefore, manufacturers should detail the correct use of the device in terms of cybersecurity and potential risks that remain. (FDA et al., 2023)

As can be concluded from the guidance documents, the focus is more on the ability of manufacturers to identify potential risks associated with their advice and how to mitigate these risks, instead of setting baseline requirements to which they should adhere.

However, these guidance documents are only meant to be advisory to the manufacturers, and not enforced by law. Yet, failure to adhere to the recommendations may lead to a prolonged approval procedure and sanctions for unsafe products. Moreover, these guidance materials have a restricted scope. They do not assess the risk assessment methodology utilised by manufacturers to evaluate the threats their products face, nor do they provide manufacturers with criteria to assess the effectiveness of the measures aimed at countering those threats. (Yuan et al., 2018)

To conclude, the exact cybersecurity requirements set out by the FDA remain fuzzy, due to the authority the FDA holds over the approval process. Additionally, the focus lies on the cybersecurity of medical devices and, therefore, the precautions manufacturers should follow, instead of procurement itself. However, this could still influence the procurement in Dutch hospitals, because when a device is sold in both markets, the hospital can be assured that the device will most likely receive timely security patches throughout its lifecycle, for example. Next to this, the device will most likely also follow the other cybersecurity requirements, which could influence the decision-making process of procuring new medical devices in the Netherlands.

3.2.2 Health Insurance Portability and Accountability Act

The Health Insurance and Accountability Act (HIPAA) passed in 1996 to draft uniform standards for exchanging electronic health information (Baumer et al., 2000). As a part of this, additional requirements were set for protecting patient privacy and security for medical data (Fedorowicz & Ray, 2004). These requirements set a federal minimum to which health organisations need to adhere to (Annas, 2003). This means that other federal or state laws can prove to be more stringent and, in that case, govern. The U.S. Department of Health and Human Services (HHS) was tasked with drafting the different policies so that the different organisations affected can comply with HIPAA (Baumer et al., 2000). Of these policies the privacy, security, and breach notification rules are most closely related to cybersecurity, and therefore will be briefly discussed below.

HIPAA Privacy Rule

The privacy rule sets standards for the protection of health information of an individual, whilst ensuring the flow of health information needed to provide healthcare. Therefore, it balances the use of information with the privacy of an individual seeking care. The privacy rule affects all insurers and healthcare providers in the US who transmit health information. It includes all "individually identifiable health information", independent of the way it is transmitted, be it electronically, via paper, or orally. Individually identifiable health information covers all demographic data, as well as physical or mental health or condition, the provision of care to the individual, and all payments for the provisioned care. This information may not be used or transmitted unless the individual requests this in writing, or if one of the six permitted disclosures applies. Next to this, when health information is used, only the minimum necessary to achieve the goal may be used, disclosed, or requested. (U.S. Department of Health and Human Services, n.d.-b)

Next to these general requirements, there are also administrative requirements that need to be followed. These require organisations to have privacy policies, procedures, and personnel in place to make sure they comply with the HIPAA. Next to this, the workforce needs to follow training on privacy rules as well. Third, the organisation needs to have suitable administrative, technical, and physical safeguards in place to limit the unlawful use of information and mitigate the effect in case it does still happen. Therefore, cybersecurity measures are also considered by the HIPAA, to limit the unlawful use of information by third parties. (U.S. Department of Health and Human Services, n.d.-b)

HIPAA Security Rule

The security rule is a comprehensive framework of US national security standards. These standards are designed to safeguard specific health information stored or transmitted electronically. By describing both technical and non-technical safeguards, the Security Rule translates the privacy protections outlined in the privacy rule. It mandates that organizations must implement measures to secure individuals' electronic protected health information (e-PHI). Specifically, organisations should safeguard the CIA of all e-PHI they create, receive, transmit, or maintain, identify potential threats, and protect against them, safeguard against foreseeable unauthorized uses or disclosures, and make sure that the workforce complies with the rule. (U.S. Department of Health and Human Services, n.d.-c)

The HIPAA is not specific on which security measures to use exactly, instead it requires organisations to consider the posed risk to e-HPI, the cost of security measures and its own technical and organisational structure. To properly identify potential risks for e-HPI, the organisation should perform a structured risk analysis, but HIPAA leaves it up to the organisation how they perform such an analysis. In terms of "technical safeguards", the organisation must implement access, audit, and integrity controls as well as data transmission security measures. Similarly to the privacy rule, the security rule also imposes different administrative requirements. These require organisations to have security management processes, information management policies and security personnel in place. Additionally, the workforce should follow training before they are authorised to access e-HPI. (U.S. Department of Health and Human Services, n.d.-c)

HIPAA Breach Notification Rule

Under the breach notification rule, organisations are required to provide a notification of a breach of protected health information. A breach can be defined as "an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information" (U.S. Department of Health and Human Services, n.d.-a). In most cases organisations will have to notify the individual, the media, and the Secretary of the HHS within 60 days after the breach. The notification should contain, as much as possible, a concise overview of the breach, details about the compromised information, guidance for affected individuals to safeguard themselves, a summary of the actions the organisation is taking to investigate, mitigate harm, and prevent breaches in the future, along with contact details of the organisation. This relates to cybersecurity, as organisations need to reflect on how it went wrong and how they can improve their security measures to prevent a breach in the future. (U.S. Department of Health and Human Services, n.d.-a)

In conclusion, the HIPAA is somewhat related to the EU's GDPR in the sense that they both focus on protecting personal information. Of these rules, the security and breach notification rule are most likely to influence the procurement of medical in the Netherlands, although limited. First, the security rule imposes some minimal requirements of cybersecurity for devices. These requirements could also translate to the Netherlands when manufacturers decide to offer the same device in both markets. Second, the breach notification rule could aid Dutch hospitals in mitigating security risks in the future and can inform their future procurement decisions.

3.3 International Medical Device Regulators Forum

The International Medical Device Regulators Forum (IMDRF) is a group of international medical device regulators that, on a voluntary basis, work on harmonising and converging international regulations for medical devices (IMDRF, n.d.). Established in 2011, the IMDRF currently consists of medical device regulatory authority representatives from Australia, Brazil, Canada, China, the EU, Japan, the US, and the World Health Organization (WHO) (IMDRF, n.d.). Their goal is to "strategically accelerate international medical device regulatory convergence to promote an efficient and effective regulatory model for medical devices that is responsive to emerging challenges in the sector while protecting and maximizing public health and safety" (IMDRF Management Committee, 2020, p. 3).

One of the regulations the IMDRF aims to harmonise is on cybersecurity. Therefore, the Medical Device Cybersecurity Working Group of the IMDRF has drafted several principles and best practices for manufacturers, regulators, and users to follow in the context of medical device cybersecurity (Medical Device Cybersecurity Working Group, 2020). Four general principles are discussed in this document: the need for global harmonisation, the consideration of cybersecurity throughout the Total Product Life Cycle (TPLC), the shared responsibility between all associated stakeholders, and the need for effective information sharing of potential risks and remedies. Besides these general principles, the IMDRF also proposes several pre- and post-market considerations for medical device cybersecurity. These will be discussed below.

3.3.1 Pre-market considerations

The IMDRF discusses five different pre-market considerations: security by design, risk management strategies, security testing, provisioning of information and documentation that allows for secure operation of the device and having a post-market plan in place (Medical Device Cybersecurity Working Group, 2020).

> *Consideration 1: security by design*
> Potential cybersecurity threats should be identified and addressed at very beginning of the design stage of a medical device, for example by utilising threat modelling. Besides this, manufacturers should consider relevant security standards to determine requirements. Finally, the IMDRF also mentions seven design principles that should be considered for optimal security: secure communication, data protection, device integrity, user authentication, software maintenance, physical access to the device, reliability and availability. (Medical Device Cybersecurity Working Group, 2020)
>
> *Consideration 2: risk management strategies*
> Appropriate risk management strategies addressing cybersecurity and safety should be in place throughout the TPLC of the device. There is not one set strategy for risk management, as numerous exist, but it should at least consist of identifying and assessing potential risks, assessing remediations, and communicating those risks. In the case of cybersecurity for medical devices, risks should be analysed by assessing the exploitability of the vulnerability and the severity of the potential patient harm when this vulnerability is exploited. (Medical Device Cybersecurity Working Group, 2020)

Consideration 3: security testing
Security testing entails that the manufacturer tests the code of the medical device on known vulnerabilities and if the security controls are effective. Testing should consider the context of the intended use of the device and its environment. One way of testing security is by simulating a potential cyberattack on the medical device. (Medical Device Cybersecurity Working Group, 2020)

Consideration 4: provisioning of information and documentation
To ensure that the device is used in a correct and secure manner, proper documentation and information should be provided. Information to be shared includes labelling of cybersecurity capabilities, technical security documentation for customers, and a summary of the cybersecurity efforts for regulators. Besides this, the risk management strategies and the post-market plan should be shared as well. (Medical Device Cybersecurity Working Group, 2020)

Consideration 5: post-market plan
As threats will evolve throughout the TPLC of the device, a plan should be in place from the pre-market stage onwards to monitor, identify, and address potential threats. This plan should include (1) a way to proactively monitor and identify new vulnerabilities; (2) a process to disclose these new vulnerabilities; (3) a way to remediate the vulnerability and update software; (4) a recovery plan after a cybersecurity incident has occurred; and (5) participation in information sharing. (Medical Device Cybersecurity Working Group, 2020)

3.3.2 Post-market considerations

As vulnerabilities change over time, several precautions should be taken to ensure security. At the post-market stage several stakeholders, such as manufacturers, users, and regulators, are involved. The IMDRF mentions six post-market considerations: the intended use environment, information sharing, coordinated vulnerability disclosure, vulnerability remediation, incident response, and legacy devices (Medical Device Cybersecurity Working Group, 2020):

Consideration 1: the intended use environment
Healthcare providers and other end users should ensure that the medical device can operate in a secure environment. They can achieve this by adopting a risk management system, adhere to cybersecurity best practices, and organising (security) training for all users of the device. On the other hand, manufacturers are encouraged to collaborate with end users to ensure optimal use and configuration of their medical devices.

Consideration 2: information sharing
Information on cybersecurity threats, vulnerabilities, and incidents should be shared freely with anyone who requires that information. When sharing, it should be noted that the information that is shared should be meaningful, consumable, and actionable for different stakeholders.

Consideration 3: Coordinated Vulnerability Disclosure
Coordinated Vulnerability Disclosure (CVD) is a method to establish "formalized processes for obtaining cybersecurity vulnerability information, assessing vulnerabilities, developing mitigations and compensating controls, and disclosing this information to various stakeholders—including customers, peer companies, government regulators, cybersecurity information sharing organizations, and the public" (IMDRF Management Committee, 2020, p. 23). This allows end users to make better informed decisions to protect their cyber assets. It should be noted that all participating stakeholders should have the opportunity to contribute to the CVD.

Consideration 4: vulnerability remediation
Vulnerability remediation must be supported by end users, manufacturers, and regulatory bodies in order to work. Manufacturers should identify and monitor potential risks, including those in third-party components. After that, they should offer a remediation and communicate about it. Regulatory bodies should cooperate with manufacturers to ensure fast approval of the remediation or update. Finally, end users should be able to incorporate the remediation in an efficient manner, be it an update or something else. If all stakeholders cooperate and act fast, the vulnerability can be solved quickly.

Consideration 5: incident response
In the case a cybersecurity related incident does take place, a detailed incident response plan should be put in place by the manufacturer and the end user. In this plan, it should be detailed how to respond to an incident, including roles and responsibilities. Next to this, incident response should be practiced and evaluated on a regular basis through training sessions.

Consideration 6: legacy devices

Finally, when a medical device reaches the end of its TPLC, it becomes a legacy device. To account for this, manufacturers should already address the end-of-life during the design phase of the medical device and should also clearly communicate the end-of-life of devices to end user. On the other hand, end users should prepare themselves for the end of support from manufacturers and should have the appropriate measures in place to mitigate any potential risk associated with the lack of support from the manufacturer.

To conclude, the policies proposed by the IMDRF mostly align with policies set out in the US and the EU, but not completely. Next to this, it mostly focusses on medical device cybersecurity, instead of implementation and procurement. Yet, it still is applicable to hospitals, as they should make sure that the device can operate in a secure manner and should remedy any vulnerability. This too can inform procurement decisions to choose for a specific device that better aligns with the hospital's cybersecurity policies or that is already proven to be safer.

3.4 Medical procurement

This section will focus on policies or regulations directly affecting the procurement process in Dutch hospitals.

3.4.1 NEN7510

As mentioned earlier, the NEN7510 norm focusses on information security in the Dutch healthcare sector (NEN, 2017). Part of this norm focusses on the procurement of new information systems and supplier relations, which both affect the procurement process. Therefore, this section will specifically focus on these two aspects of the NEN7510 norm, as they will need to be followed by all hospitals that follow this norm.

The NEN7510 norm provides detailed information on what could be considered during the procurement of new information systems. However, not everything is obligatory for hospitals to follow, they are mere pointers of what could be considered (NEN, 2017). Therefore, Table 4 below provides an overview of the high-level requirements set by the NEN7510 norm, without going too much into detail of what hospitals could consider fulfilling these requirements.

Table 4 - NEN7510 procurement requirements, based on NEN (2017)

Req. num.	*Requirement description*
Part 1: Procurement requirements	
Part 1.1: Security requirements for information systems	
1.1.1	(Cyber)security requirements for new IT solutions, or expansion of current IT solutions should be set at the start of the procurement process and analysed during the process of selection.
	1.1.1.1 IT solutions that process personal health information should be able to uniquely identify a patient and merge any potential double files made for the same patient.
	1.1.1.2 IT solutions should provide caregivers with the right information to verify that the information belongs to the patient they are providing care to.
1.1.2	Information transmitted on public networks should be protected against fraudulent activities, contract dispute with suppliers, and unauthorised publication or alteration of data.
1.1.3	Information that is part of a database transaction should be protected from incomplete transmission, incorrect routing, unauthorized modification of messages, disclosure, duplication, or playback.
	1.1.3.1 Publicly available health information should be archived with accreditation of the author and its integrity protected.
Part 1.2: Security in development and support processes	
1.2.1	Prior to the development of information systems, security rules should be determined and adhered to throughout the development process. This includes both the security of the to-be developed information system, as well as the security of the development process.
1.2.2	The introduction of new systems and significant changes to existing systems should follow a formal process of documentation, specification, testing, quality control and managed implementation. This to ensure that current cybersecurity measures are not compromised.
1.2.3	When operating systems are changed, critical processes should be evaluated and tested to ensure no negative consequences for the activities and cybersecurity of the organisation.
1.2.4	Off the shelf software should not be altered or altered as little as possible to ensure proper (secure) functioning and easy updates by the developer.

1.2.5	Internal engineering projects of secure systems should follow documented procedures based on the principle of secure engineering. These procedures should be evaluated frequently. When these systems are outsourced, the same procedures should be applied.
1.2.6	A secure development environment should be set up for the development and/or integration of critical systems. This secure development environment encompasses all people, processes, and technologies associated with the development and/or integration of new systems.
1.2.7	When system development is outsourced, the development process should be supervised and monitored by the organisation. This also includes the consideration of licensing agreements, ownership of source codes, accepted risks, the possibility to audit development processes and countermeasures, and the results of security tests.
1.2.8	Throughout development security measures should be independently tested.
1.2.9	New systems, upgrades to systems, or updates, should be tested and evaluated prior to installation. In particular, requirements 1.1, 1.2, and 1.4 should be considered during the tests and evaluation. These tests should be performed in a realistic testing environment.
1.2.10	Data used during testing and evaluation of new systems should be carefully selected, protected, and checked. The use of operational databases that include personal or other sensitive information should be avoided.
Part 2: Supplier relation requirements	
Part 2.1: Information security in supplier relations	
2.1.1	Security requirements should be set and documented in accordance with the supplier when they have access to organisation assets. This to minimise security risks. These requirements could entail incident management, minimum cybersecurity requirements per type of data, and awareness training.
2.1.2	All relevant cybersecurity requirements should be set and agreed upon in a contract with suppliers that have access to the organisation's IT infrastructure, or that process, store, communicate, or offer data to the organisation.
2.1.3	Supplier contracts should incorporate requirements for information security risks in the supply chain of IT services and products.
Part 2.2: Supplier service management	
2.2.1	Organisations should monitor, evaluate, and audit supplier services frequently.
2.2.2	Organisations should be prepared for changes in supplier services. In particular, the service agreement and changes in the services they offer (e.g. the use of new technologies).

To conclude, the NEN7510 norm proposes quite detailed requirements hospitals should consider during the procurement of new medical devices, as can be seen in the table above. Although the NEN7510 norm is not compulsory to follow, it is almost standard practice for hospitals to do so. Therefore, the implications for the procurement process in Dutch hospitals are quite extensive.

3.4.2 Tendering law

Tender law focusses on the process of awarding a public contract to a company. Its goal is to ensure value for taxpayer's money, prevent corruption, and promote innovation. In the EU this is governed via EU directive (2014/24/EU), which is transposed in the Netherlands as the 'Aanbestedingswet 2012', which was last updated in 2022 (Aanbestedingswet 2012, 2022).

All contracting authorities that are publicly funded, or governed by public law are obliged to follow tendering law. This means that for example governmental bodies, universities, and utility providers are included. This leaves an interesting discrepancy in the healthcare sector, as academic hospitals are also universities, whilst non-academic hospitals are not. This means that academic universities are obliged to follow tendering law, whilst non-academic hospitals are not obliged to do this. (Bruggeman et al., 2010)

Not everything a contract authority buys must be publicly tendered, as there is a threshold value for the amount procured. The threshold for national tendering is not defined in the 'Aanbestedingswet 2012', however a threshold for €50,000 for goods and €1 million for works is very common in the Netherlands. If this threshold is passed, the tender only has to be put out within the Netherlands. There is also an EU threshold of €221,000 for goods and €5.548 million for works. If this threshold is passed, the tender must be put out within the whole EU. After the tender is put out, economic operators can submit their bid to the contracting authority. Hereafter the contracting authority evaluates the bids and chooses one economic operator. This evaluation must follow the four principles of tendering law. First, the principle of nondiscrimination ensures that all economic operators must be considered, regardless of their country of origin or language. Second, the principle of equal treatment states that all economic operators must be treated equally, regardless of whether one is an old friend, for example. Third, the principle of transparency allows all parties to verify the actions and decisions of the contracting authority. Last, the principle of proportionality dictates that the requirements set for the tender must be proportional to the contract that is awarded. (Bruggeman et al., 2010)

To conclude, tendering law only affects academic hospitals. However, it does impact them significantly as for most medical devices they will be required to put out a public tender and defend their decision publicly. This adds several extra steps to the procurement process that non-academic stakeholders do not have to follow.

3.4.3 Convenant Medische Technologie

The Convenant Medische Technologie (2016), or in English the 'Covenant Medical Technology' is a document set up by the Dutch healthcare sector to ensure safe use of medical technology. Part of this covenant are guidelines for the procurement of medical devices. Yet, these guidelines are not stringent.

Prior to the start of the procurement process, the hospital needs to document the following: the need for procurement, the program of requirements, a risk analysis, competency requirements and relevant training for medical and technical staff, and a plan for periodic evaluations. This needs to be stored for each procurement process started in the hospital. For the procurement process itself, hospitals should have a documented procedure in place that involves all relevant stakeholder backgrounds. Finally, a plan should be in place for periodic replacement of medical devices within the hospital.

3.5 Answering sub question 1

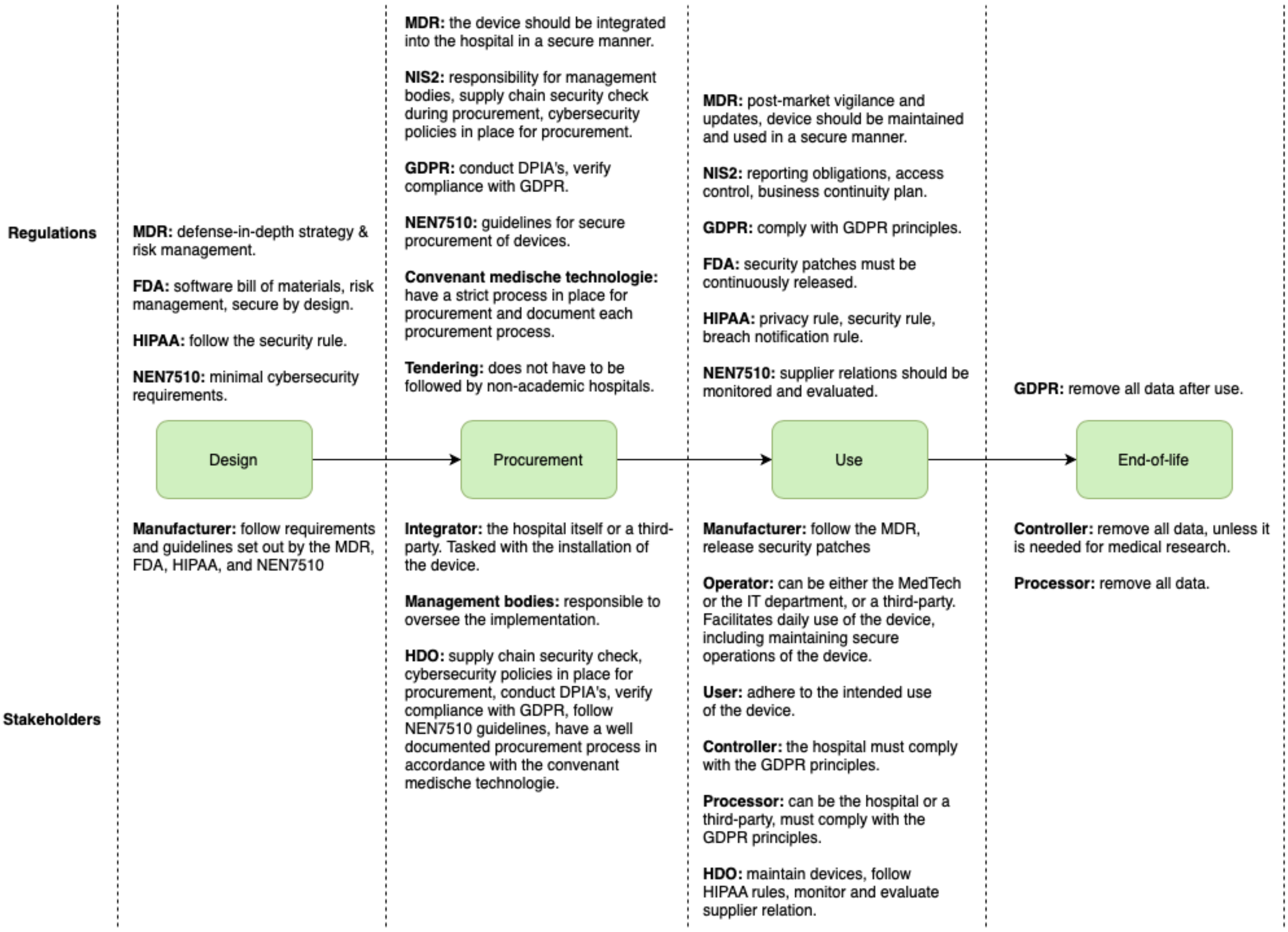
This section will provide an answer to SQ1: *How are cybersecurity considerations included in the current regulations and standards governing medical devices and the procurement thereof?* Table 5 below provides an overview of all regulations discussed in this chapter and the implications they have on both the procurement of medical devices and cybersecurity.

Table 5 - Overview of the institutional environment

Regulation	*Procurement implication*	*Cybersecurity implication*
MDR	Procurement is indirectly influenced, as the integrator needs to make sure that the new medical device can securely operate in its intended environment.	The MDR poses quite some cybersecurity requirements on manufacturers specifically which must adhere to specific pre- and post-market activities to ensure cybersecurity. The operator is tasked with ensuring cybersecure operation throughout the lifecycle of the device, including installing security patches.
NIS2	NIS2 impacts procurement in two ways. First, it obliges entities to assess the cybersecurity of their suppliers and service providers, adding an extra step to the procurement process. Second, policies should be in place that manage and define IT security during the procurement process.	The cybersecurity implications are significant, for both the manufacturer and the hospital. Although the focus of NIS2 lies, in this specific case, on hospitals, manufacturers also need to adhere in order for them to sell their device. Requirements include patch management, cryptography, multi-factor authentication, and more.
GDPR	The GDPR only slightly impacts the procurement process. It only applies as such that all medical devices, or other services procured need to comply with the GDPR, which should be checked during the procurement process.	The cybersecurity measures focus solely on data protection and privacy of individuals and are limited. Hospitals and manufacturers are required to consider the state-of-the-art in terms of cybersecurity, but are not obliged to implement this, as costs should weigh up to the benefits. Therefore, the exact implications remain uncertain.

FDA	The FDA has no specific procurement guidelines. Procurement in the Netherlands could only be influenced in the sense that devices sold in both markets also adhere to the FDA's cybersecurity standards, which could influence the decision.	The exact cybersecurity implications remain fuzzy, as the FDA mostly relies on so called guidance documents, instead of true requirements. The main implication for cybersecurity is the PATCH act, which mandates that manufacturers should provide security patches throughout the lifecycle of a device. The guidance documents focus on security-by-design and risk analyses that manufacturers could follow prior to their approval application.
HIPAA	There are no direct procurement implications. The breach notification rule may only inform hospitals in the Netherlands about certain vulnerabilities, which might influence their decision.	In terms of cybersecurity, the implications are somewhat similar to the GDPR, as they focus on protecting information. There are no set requirements to do so, instead organisations should perform a risk analysis and base their security measures on that.
IMDRF	The only procurement implication is that the device should be able to operate safely in its intended use environment. Otherwise, there are no clear rules for procurement.	Cybersecurity requirements focus on risk analyses, security testing, security-by-design, and post-market activities to maintain the security. However, no concrete minimum requirements are mentioned.
NEN7510	The NEN7510 norm provides detailed information on what could be considered during the procurement of new IT systems or medical devices. However, they are pointers for what could be considered and not everything is obligatory. The main focus lies on ensuring the security of IT systems and how they were developed as well as how relations with suppliers should take shape.	The security implications from the NEN7510 norm mainly focus on information security. Requirements include things such as security testing, a secure development environment, protected information transmissions, supplier cybersecurity evaluation, and more.
Tendering	Overhauls the procurement process for academic hospitals, as they will need to put a tender out publicly, before being able to procure new devices.	None.
Convenant Medische Technologie	Requires hospitals to properly document the procurement processes they have in place. Additionally, a plan should be in place to periodically replace the devices in use within a hospital.	None.

To deepen the understanding of how these regulations impact the lifecycle of a medical device, Figure 5 below disseminates the previously discussed regulations over four distinct phases: design, procurement, use, and end-of-life. Above these phases the implication of each regulation on that specific phase is summarised. Below it, the stakeholders that are targeted by the regulations are discussed. The IMDRF is left out of this figure, as to improve the clarity. The IMDRF is not a regulation of itself, but rather a guideline for regulators. Therefore, it does not directly impact the current healthcare sector and is left out of this figure. A HDO refers to a Healthcare Delivery Organisation, in this case the hospital.



MDR: defense-in-depth strategy & risk management.

FDA: software bill of materials, risk management, secure by design.

HIPAA: follow the security rule.

NEN7510: minimal cybersecurity requirements.

MDR: the device should be integrated into the hospital in a secure manner.

NIS2: responsibility for management bodies, supply chain security check during procurement, cybersecurity policies in place for procurement.

GDPR: conduct DPIA's, verify compliance with GDPR.

NEN7510: guidelines for secure procurement of devices.

Convenant medische technologie: have a strict process in place for procurement and document each procurement process.

Tendering: does not have to be followed by non-academic hospitals.

MDR: post-market vigilance and updates, device should be maintained and used in a secure manner.

NIS2: reporting obligations, access control, business continuity plan.

GDPR: comply with GDPR principles.

FDA: security patches must be continuously released.

HIPAA: privacy rule, security rule, breach notification rule.

NEN7510: supplier relations should be monitored and evaluated.

GDPR: remove all data after use.

Manufacturer: follow requirements and guidelines set out by the MDR, FDA, HIPAA, and NEN7510

Integrator: the hospital itself or a third-party. Tasked with the installation of the device.

Management bodies: responsible to oversee the implementation.

HDO: supply chain security check, cybersecurity policies in place for procurement, conduct DPIA's, verify compliance with GDPR, follow NEN7510 guidelines, have a well documented procurement process in accordance with the convenant medische technologie.

Manufacturer: follow the MDR, release security patches

Operator: can be either the MedTech or the IT department, or a third-party. Facilitates daily use of the device, including maintaining secure operations of the device.

User: adhere to the intended use of the device.

Controller: the hospital must comply with the GDPR principles.

Processor: can be the hospital or a third-party, must comply with the GDPR principles.

HDO: maintain devices, follow HIPAA rules, monitor and evaluate supplier relation.

Controller: remove all data, unless it is needed for medical research.

Processor: remove all data.

Figure 5 - Regulations detailed over a medical device's lifecycle

Figure 5 paints a clear picture what each stakeholder needs per phase according to the regulations. However, it does not show which regulation targets which stakeholder. Therefore, Figure 6 shows which stakeholders are affected by the regulations discussed in this chapter, in the context of cybersecurity. Here again, HDO includes hospitals when regulations did not specify a specific stakeholder group. In addition, third parties cover a wide variety of stakeholders, including the manufacturer, but also for example contractors. For a better definition of who is targeted by these regulations, please refer back to chapter of that regulation.

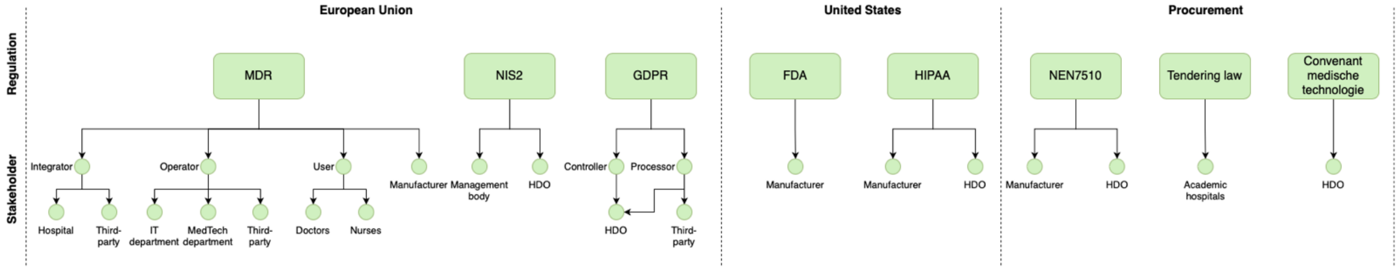


Figure 6 - Stakeholders targeted per regulation

From the table and figures, it can be concluded that only two policies directly impact the procurement of new medical devices for all hospitals: the NIS2 and NEN7510. Both focus on assessing the security practices of suppliers during the procurement process, as well as having certain minimum cybersecurity requirements in place. Next to this, tendering law requires academic hospitals to put out public tenders when they procure new medical devices, therefore shaping their procurement process to a certain extent. However, other regulations can influence the procurement process indirectly, either by informing hospitals about certain vulnerabilities, by obliging them to make sure the device can operate in a secure environment, or by ensuring that the devices they buy are secure. Yet, whether these regulations in fact indirectly influence the procurement process remains unsure.

Yet, the cybersecurity implications that are derived from these different policies are bigger with different requirements set for both manufacturers and hospitals. Most requirements centre around risk analyses that must be performed that consider the state-of-the-art. This keeps the exact implications uncertain, as it is up to the discretion of hospitals and manufacturers to perform their own risk analyses. However, the MDR, NIS2, FDA, and NEN7510 do specify some concrete requirements, such as patch management, cryptography standards, secure development environment, and more.

In addition, most regulations focus on either the manufacturers, the hospitals, or both. Some regulations, such as the GDPR and the MDR, specifically mention that third parties performing tasks on behalf of the hospital must also comply with these regulations, whilst others don't. NIS2 places additional emphasis on the management bodies of hospitals, setting specific requirements for them.

Therefore, it can be concluded that the focus for regulators mainly lies on ensuring basic cybersecurity standards in medical devices, instead of requiring certain standard practices in the procurement process. However, this might change when NIS2 is transposed into Dutch law and the procurement requirements stay the same. Yet, this has still to take place.

4 The procurement process of medical devices

This chapter will focus on detailing the current procurement processes of medical devices in Dutch hospitals. This was analysed by conducting semi-structured interviews with different stakeholders from hospitals in the Netherlands. These interviews were then utilised to perform a framework analysis to compare the different hospitals. Therefore, first the participant population of this study is detailed. Thereafter, the framework synthesised from the interview data is elaborated upon. Third, the results of this study, put into context of the framework, are discussed. Finally, an answer is provided to SQ2: *What are the existing general procurement practices for medical devices in hospitals in The Netherlands?*

4.1 Participant population

Purposive sampling was used to gather participants for this study, as participants should have specific knowledge to participate in this study (Bryman, 2016). Purposive sampling can be divided into the sampling of context and the sampling of participants. Both are elaborated upon below.

In terms of the context, a specific sample was set on hospitals within the Netherlands. Both academic and non-academic hospitals were considered at this time. This way the sample size could be as large as possible, which was needed because of the time constraint of this study and the associated response rate. However, based on the initial results of this study and the response rate, the sample context was shifted towards non-academic hospitals within the Netherlands, as these had a higher response rate, and the initial results showed a large difference between academic and non-academic hospitals in terms of procurement. This differentiation is elaborated upon in section 4.3. The hospitals that participated in this study are detailed in Table 6 below.

Table 6 - Overview of participating hospitals

Hospital ID	*Location*	*Type*	*# of beds*
1	The Netherlands	Non-academic	0 - 499
2	The Netherlands	Non-academic	1000 - 1499
3	The Netherlands	Non-academic	500 - 999

The selection of participants within these hospitals was based on criterion sampling, as participants must be knowledgeable on the topic (Bryman, 2016). Criteria included: 1) the participant should be knowledgeable on procurement processes in hospitals, and 2) the participant should have contributed to procurement processes at their current hospital for at least two years, to ensure a certain experience and degree of comparability between different processes.

Based on these criteria, an initial 15 participants were contacted across 9 different hospitals. 8 potential participants answered, of which 4 participated in this study. This results in a response rate of 53,33% and a success rate of 26,67%. To increase the participant count and include the views of more stakeholders on the same procurement processes, snowball sampling was used. After each interview, participants were asked if they could refer to a colleague that fulfil the two criteria. This resulted in two additional participants for this study. An overview of the participants from within hospitals can be found in Table 7 below.

Table 7 - Hospital stakeholders interviewed

Hospital ID	*Participant ID*	*Combined ID*	*Role*	*Experience*	*# procurements*
1	1	H1.P1	Procurement / IT	2 years	~ 12
1	2	H1.P2	Medical	14 years	~ 13
2	1	H2.P1	Clinical physician	8 years	~ 50
2	2	H2.P2	IT	20 years	~ 9
3	1	H3.P1	Clinical physician / procurement	20 years	~ 100
3	2	H3.P2	Medical	8 years	~ 4

In total six interviews with hospital stakeholders were conducted. The average duration of these interviews was 41:33 minutes. Participants were asked about their experiences with the procurement process at their hospital, based on a semi-structured interview protocol. Questions included how the procurement process looks like at their hospital, but also how cybersecurity is considered during this process. The full interview protocol used during the hospital stakeholder interviews can be found in Appendix A.1.

4.2 Thematic framework

This section follows the first two steps of a framework analysis: 1) data familiarisation and 2) identifying a thematic framework. As mentioned in chapter 2.3, the first step consists of familiarising with the data at hand and identifying major themes. This was done by going over the first two interview transcripts of this study and assigning preliminary codes to the data. This resulted in a total of 56 different codes.

In the second step, the concrete descriptions of themes found in the initial 56 codes are merged into more abstract concepts as to provide a framework on which the other interviews can be analysed. This was done by merging the 56 codes into six major themes, aligned with the different sub questions of this study. However, the initial 56 codes were not deleted, but rather function as individual sub-themes of each major themes. The six major themes are described in Table 8 below.

Table 8 - Thematic framework overview of the procurement process

Theme	*Description*	*# of sub-codes*
Procurement process	This theme entails all steps taken or procedures followed during the procurement of medical devices in hospitals. Its subthemes focus on one step or procedure each. This way a comprehensive view of the procurement process is generated.	14
Requirements	The sub-themes of requirements focus on the different requirements set during the procurement of medical devices. The major goal of this study is to determine whether and how cybersecurity is one of those requirements.	11
Stakeholders	This theme focusses on the different stakeholders involved during the procurement process and the way they contribute or influence it.	10
Procurement initiation	Procurement initiation focusses on the different reasons new procurement processes are started for medical equipment.	7
Outside influences	This theme describes different outside influences on the procurement process of medical devices. Outside is hereby defined as outside of the hospital itself. This is important to know, as outside influences can steer the hospital to buy other devices.	3
Regulations	This theme focusses on the different regulations or policies hospitals follow during the procurement process, or regulation and policies that influenced the procurement of new medical devices.	7
Other	General notes and remarks made by the participants, that are related to this study.	3

As can already be partly concluded from the description table above, these themes and their sub-themes are not stand-alone. In contrary, they are often related and can support or contradict each other. Therefore, Figure 7 depicts the relations between the different main themes. Additionally, above each main theme it is shown which sub question it aids in answering. The relation 'is cause of' is used when one theme can be the reason for another reason. This is particularly used for the 'procurement initiation' and 'requirements' themes. Here, other themes can be the cause for certain requirements or the initiation of a procurement process. The relation 'is part of' is used for themes that are a part of another theme. Specifically, this is the case for the 'requirements' and 'stakeholders' theme, that both are a part of the procurement process. Finally, outside influences are associated with the procurement process, as they do not have a direct role in the procurement process but do still influence it.

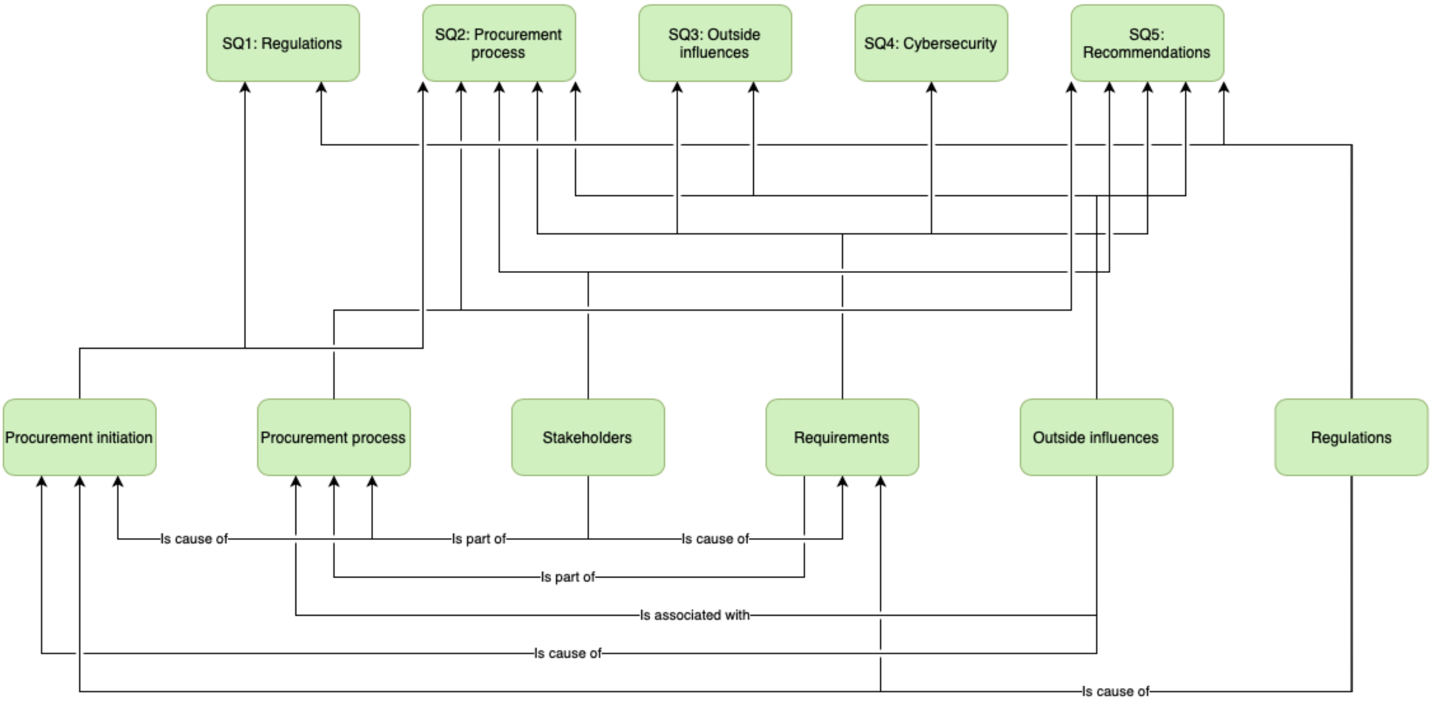
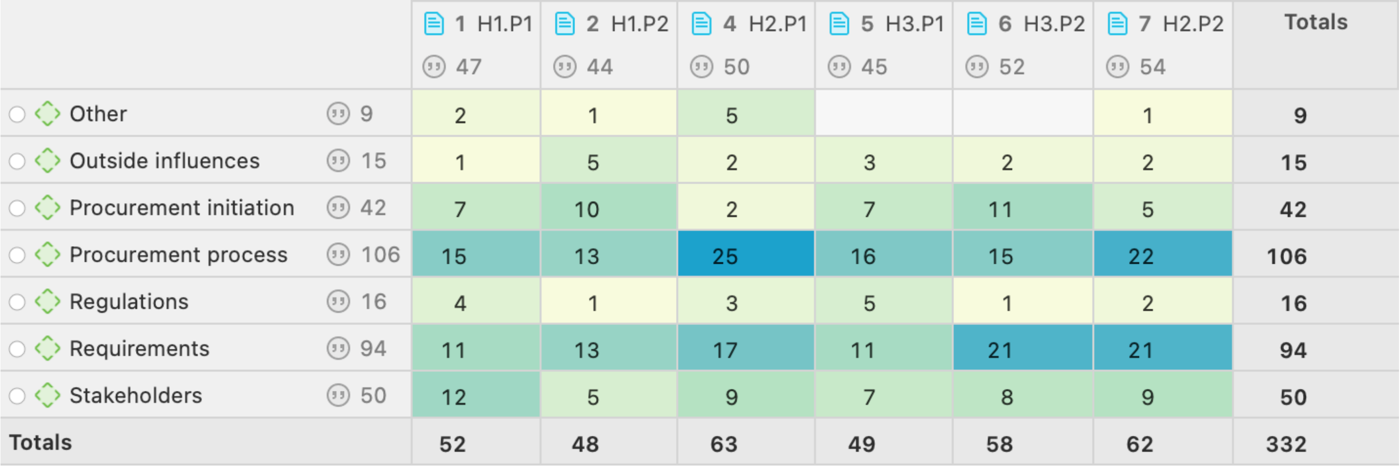


Figure 7 - Thematic framework relations

Data, or theoretical saturation occurs when new data does not lead to new dimensions of the themes found (Bryman, 2016). This was the case after coding the first four interviews of this thesis. The final two interviews with H3.P2 and H2.P2 consequently did not lead to any new sub-codes or new dimensions to existing codes. Data saturation might have been reached so quickly due to the homogenous sample and the narrow scope of the interview transcript (Bryman, 2016). This can result in a smaller variation in answers during the interviews, which aids in data saturation being reached. Additionally, Table 9 shows an export of ATLAS.ti that indicates the frequency of each main theme mentioned per interview. Additionally, the table shows the number of quotes per interview and per main theme. This shows how the codes are distributed throughout the different interviews.

Table 9 - Code distribution per theme



		1 H1.P1	2 H1.P2	4 H2.P1	5 H3.P1	6 H3.P2	7 H2.P2	Totals
		47	44	50	45	52	54	
○ Other	9	2	1	5			1	9
○ Outside influences	15	1	5	2	3	2	2	15
○ Procurement initiation	42	7	10	2	7	11	5	42
○ Procurement process	106	15	13	25	16	15	22	106
○ Regulations	16	4	1	3	5	1	2	16
○ Requirements	94	11	13	17	11	21	21	94
○ Stakeholders	50	12	5	9	7	8	9	50
Totals		52	48	63	49	58	62	332

All codes and sub-codes can be found in the codebook in Appendix C.

4.3 Discussion

This section will discuss the thematic framework as presented earlier. Specifically, this chapter will focus on the inner workings of the procurement process itself. Therefore, the ‘outside influences’ theme is not discussed in this section. For the discussion of the ‘outside influences’ theme, please see section 5.3.2. The results of all other themes are discussed below. As all interviews were held in Dutch, quotes mentioned in this chapter were translated into English.

The following sections will all discuss one of the major identified themes. The full framework analysis can be found in Appendix D.

4.3.1 Stakeholders

During the interviews, a vast number of stakeholders that contribute to the procurement process within a hospital were discussed. In total, 10 different stakeholders came forward during the interviews, which all contributed to the procurement process in their own way. How each stakeholder contributes to the procurement process will be elaborated upon below.

Clinical physicists contribute to the procurement process in several ways. First, they can initiate a procurement process when they think it is fit. Second, they set requirements for the device based on their expertise, which are mostly linked to safety and radiation of new devices. Participants from H1 mentioned that clinical physicists may also contribute to the procurement process by evaluating the servicing agreement that the manufacturer proposes. Finally, participants from H2 and H3 mentioned that they can be part of the investment committee, which will be elaborated upon in section 4.3.3.

Contract managers mostly play a role after the device has already been procured. They evaluate the servicing agreement made with suppliers in H1 and H2. H2.P1 mentioned: *“We have a supplier evaluation. We have a contract manager within our department, and he has set up a process for periodically and mutually evaluating important suppliers of ours. So, we evaluate them, but they also get the chance to assess us, so that you can achieve better cooperation, so to speak.”* This evaluation can then be used in future procurement processes.

The department head is the manager of a specific hospital department. They are often the one who start the procurement process and therefore takes the lead throughout the process. They are also part of the steering / investment committee, which will be elaborated upon in section 4.3.3.

Doctors are, of course, also part of the procurement process as they are the one who will have to work the most with the new devices. Therefore, they set more functional requirements for the devices. H2.P2 summarised that as follows: *“From a functional point of view of okay: What do we expect from the solution? What should it be able to do? What should it support us in?”* Doctors can also voice their need for a new device, which in return can be a reason to start a new procurement process. In H2, doctors can also be part of the investment committee, participants from other hospitals did not mention this. In addition, participants from H1 also mentioned nurses as a stakeholder group that can contribute to the program of requirements, as they too will have to work with some of the devices being procured. Nurses were not mentioned by participants from the other two hospitals.

Of course, no devices can be procured without the allocation of the necessary funds. Therefore, someone who is financially responsible for the hospital is also part of the procurement process to allocate the funds. In H1 this is done directly by someone from the finance department, whilst in H2 and H3 this is done through the investment committee.

Each hospital also has someone who specialises in infection prevention and the cleanability of devices. Therefore, based on their expertise and knowledge, they contribute to the program of requirements to ensure hygienic operations of the device. H1.P1 mentioned: *“(...) someone from infection prevention will look at how we can clean this and ensure that everything stays tidy.”*

The IT department plays a role during the procurement process when the device includes an IT component, H2.P1: *“For example, if something has to do with IT, an IT supervisor will also join.”* Now that devices are becoming more and more interconnected, the IT department joins the procurement more often. They set IT and cybersecurity related requirements for the device and can evaluate the cybersecurity of devices. H1.P1 mentioned that the IT department can also initiate a procurement process, albeit not related to a device: *“[The Information Security Officer] said: Hey, pay attention, there is a new standard that we have to comply with, so we have to look for a certifying party.”* The other two hospitals did not mention this.

The medical technology (MedTech) department evaluates the reliability and serviceability of medical devices and based on this can also set requirements for the new devices. In addition, H3.P1 mentioned that they can start a procurement process when they think it is needed*: "So medical technology can indicate: these devices must in any case be replaced next year or we recommend replacing them. Or maybe this one is already 10 years old, but it still holds up just fine."* Additionally, it is noticeable how, because medical devices are becoming more interconnected, the medical technology department and the IT department of hospital 2 have merged. The goal of this merger was to streamline the processes of the departments, as they became more and more dependent on each other. H2.P1, as a clinical physicist within the MedTech department recalls*: "(...) for a long time we really had separate processes, where until one or two years ago it was like, you buy a device that also includes a piece of software and then we delivered it as medical technology. It was technically completely in order, but in the end the user was very unhappy, because the software had not yet been checked and rolled out and did not work at all, so to speak. (...) And with that in mind, we are increasingly integrating our processes with each other. You also see that the MedTech supervisor and the IT supervisor are working more and more closely together to see together how we ensure (...) that what we deliver also meets the wishes and requirements of the users and is the best, so to speak, total package. So, from our view IT is playing an increasingly important role in this. We are increasingly aware that we cannot do it without that branch, so to speak."*

Perhaps one of the most important stakeholders during the procurement process is the procurement department of the hospital. They are the one that are in contact with suppliers to make the final deal and negotiate the price and contract. H2.P1 specifically mentioned that for the price, they look at the total cost of ownership: *"Procurement provides advice based on the purchase cost, but also on the maintenance costs that apply. So yes, depending on the size of the device or the investment, we also look at total cost of ownership."* What is noticeable is that the procurement department of hospital 3 is outsourced to a secondary organisation that coordinates the procurement efforts of multiple hospitals simultaneously. H3.P1: *"Well, as a hospital we are affiliated with [redacted for privacy], a purchasing organization. (...) Think of it as the purchasing department of the hospital, but than of [redacted for privacy] hospitals at the same time."* Somewhat similarly, hospital 1 too collaborates with another hospital, but still has their procurement department under own control, instead of outsourcing it. H1.P1: *"We have a combined purchasing department for two hospitals. (...) With the aim of also finding some synergy in the market."* Contrary to this, hospital 2 does not seek active collaboration on the procurement of medical devices.

Finally, besides each stakeholder's main role, they can have multiple different side roles in the hospital. For example, a doctor can also be a part of the investment committee or be a department head. This adds another layer of complexity to the procurement process in hospitals.

All stakeholders within the hospital that contribute to the procurement process are depicted in Figure 8 below, including any possible relations between the different stakeholders.

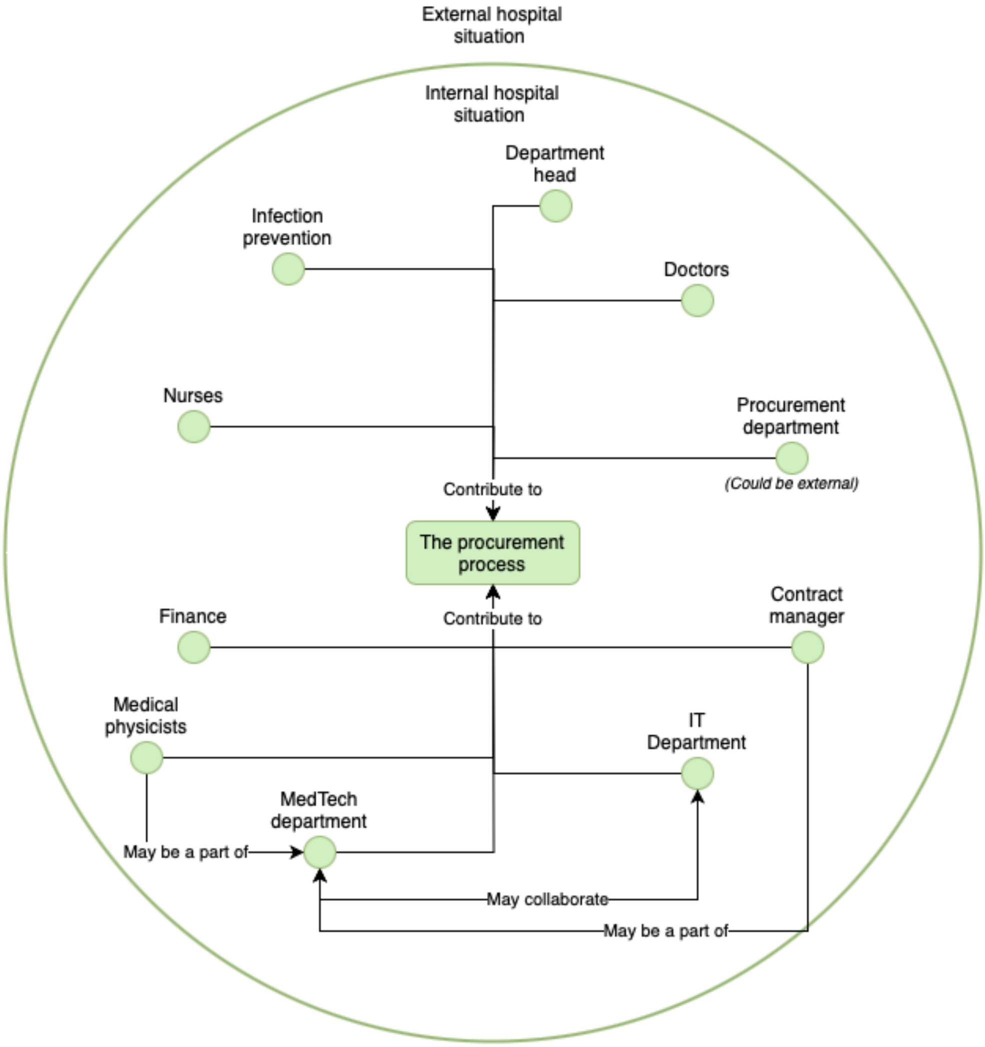


Figure 8 - Internal stakeholder analysis

4.3.2 Procurement initiation

During the interviews several reasons to initiate a new procurement process were discussed. This resulted in 7 sub-codes for this theme and 3 sub-codes from the 'Stakeholders' theme linked to this theme.

Within hospitals, the 'owner' of a medical device often starts the procurement process of a new device and can take the lead. This owner can either be a doctor that functions as a department head or a separate business manager of the department. This owner is tasked with starting the new process, but also to listen to the needs of the department. H1.P1 said: "*What you always have within the organisation is someone who is responsible for a certain piece of equipment. That is often a department head and he is also advised by supporting staff services (...).*" In addition, H2.P2 mentioned: *"Generally, a team leader starts a procurement process. So, [the team leader] from the department. For example, an ENT who says I want a new device."*

Besides the 'owner' of a medical device and its department, there are other stakeholders from within the hospital that can pitch the need for a new device. Clinical physicists, the IT department, and the MedTech department were all mentioned as stakeholders from within the hospital that might start a new procurement process when they think it is needed. For example, H2.P1, clinical physicist, mentioned: *"(...) for example, the infusion pump or the blood pressure monitor are used in so many different departments. If we go through a new procurement process, it will not be one user department that submits the request. But then we often set up the business case in advance and consult the various users for additional input than for such a business case."*

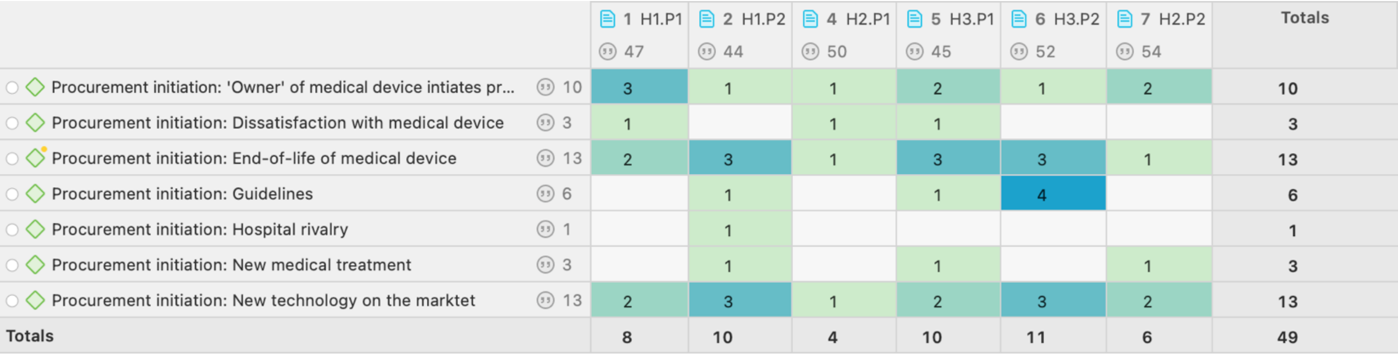
The two main reasons to start the procurement process for a new device are the end-of-life of the current medical device and the introduction of a new technology on the market. The end-of-life of a medical device often means that the device has been written off and therefore needs replacement. These replacements are done at a regular interval, for example, every 10 years. H3.P1 mentioned: *"The medical technology department may indicate: This device is going out of service, or these devices are going out of service and you must replace them."* Devices can be replaced sooner when a new technology is introduced on the market that drastically improves the current treatments offered to patients, or that improves the workflow of the medical staff. H1.P2 mentioned it as follows: *"(...) for example, that there are new ventilation techniques that certain machines can only do. So, then something new has to come that isn't there yet"*, or H3.P1: *"The user may be like, yes, I really miss certain functionalities that the newer devices have and that our device does not have."*

Additionally, the introduction of a new medical treatment can also be a reason to initiate a new procurement process, although less frequent. In contrast, the introduction of a new technology on the market discussed in the previous paragraph focusses on the improvement of current treatments. However, new treatments are not frequently introduced, so this is not often the reason to start a new procurement process. H1.P2: *"So the team says: we want to give this and this treatment. We don't have it right now, so we want that."*

Other reasons to start a new procurement process are hospital rivalry, new guidelines, and dissatisfaction with current devices. Hospital rivalry is only mentioned by H1.P2 as a reason to procure new devices to remain an attractive hospital in comparison to other hospitals. Therefore, they will remain their competitive edge: *"(...) this means you remain an attractive hospital instead of having old junk. And as doctors, when we sat at a conference with other doctors, it was a bit of a macho thing. What news do you have? Oh, you have nothing new? Well, I'll pay for dessert then."* Second, new guidelines set by the NZa (Dutch health authority), or the medical specialists association can force hospitals to replace or procure new devices. These guidelines set the standard that hospitals need to adhere to when they want to offer certain treatments. H3.P2 mentioned it as follows: "*They draw up a set of requirements stating what a hospital must meet to treat certain [redacted for privacy]. And that includes software, but also what qualities and competencies the [doctors] must have for this. Can you offer certain diagnostics 24/7? (...) How many treatments do you do per year, so to speak, so that you have sufficient expertise. All those kinds of requirements are attached to it."* These guidelines are therefore specified to improve medical treatments, and do not include cybersecurity. Finally, dissatisfaction with the current device in use can be the cause to procure a new one. However, due to financial restriction devices should still be in use for some time, before they can be replaced. H3.P1 mentioned that as follows: *"(...) the user indicates: I miss certain things that new devices can do. In theory you can say that after two years, but then you really won't get any money again, so normally the devices are at least 10 years old."*

Table 10 below is an output from ATLAS.ti that shows how often each reason to start a procurement process was mentioned per interview.

Table 10 - Code distribution procurement initiation



		1 H1.P1	2 H1.P2	4 H2.P1	5 H3.P1	6 H3.P2	7 H2.P2	Totals
		47	44	50	45	52	54	
○ Procurement initiation: 'Owner' of medical device intiates pr...	10	3	1	1	2	1	2	10
○ Procurement initiation: Dissatisfaction with medical device	3	1		1	1			3
○ Procurement initiation: End-of-life of medical device	13	2	3	1	3	3	1	13
○ Procurement initiation: Guidelines	6		1		1	4		6
○ Procurement initiation: Hospital rivalry	1		1					1
○ Procurement initiation: New medical treatment	3		1		1		1	3
○ Procurement initiation: New technology on the marktet	13	2	3	1	2	3	2	13
Totals		8	10	4	10	11	6	49

From this table, based on how often each reason was mentioned during the interviews, it can be concluded that the end-of-life of medical devices and the introduction of new technology on the market are the primary reasons to initiate a procurement process. Both reasons were mentioned 13 times during the interviews and by all participants. This is followed by, with some distance, the introduction of new guidelines the hospitals need to adhere to. The introduction of new medical treatments and dissatisfaction with current medical devices were both mentioned 3 times. This can be explained by the fact that new treatments are not put onto the market frequently, and because even though the user might be dissatisfied with the current device, new funds are not always available which would result in the need to wait for the end-of-life of the device. Finally, as previously mentioned, hospital rivalry was only mentioned by H1.P2.

4.3.3 Procurement process

Each participant described the procurement process they follow within their hospital. This resulted in sub-codes that define process steps and sub-codes that mention other factors of the procurement process. How these sub-codes came forward during the interviews, can be seen in the full framework analysis of the 'procurement process' theme in Appendix D. The process steps and other factors are discussed and elaborated upon below.

What can be concluded from the interviews and the framework analysis is the striking resemblance between the procurement processes of the different hospitals. This resulted in a general overview of the procurement process in hospitals, shown in Figure 9. Although marginal differences still exist between hospitals, they all resemble this general structure. The process will be elaborated upon below this figure.

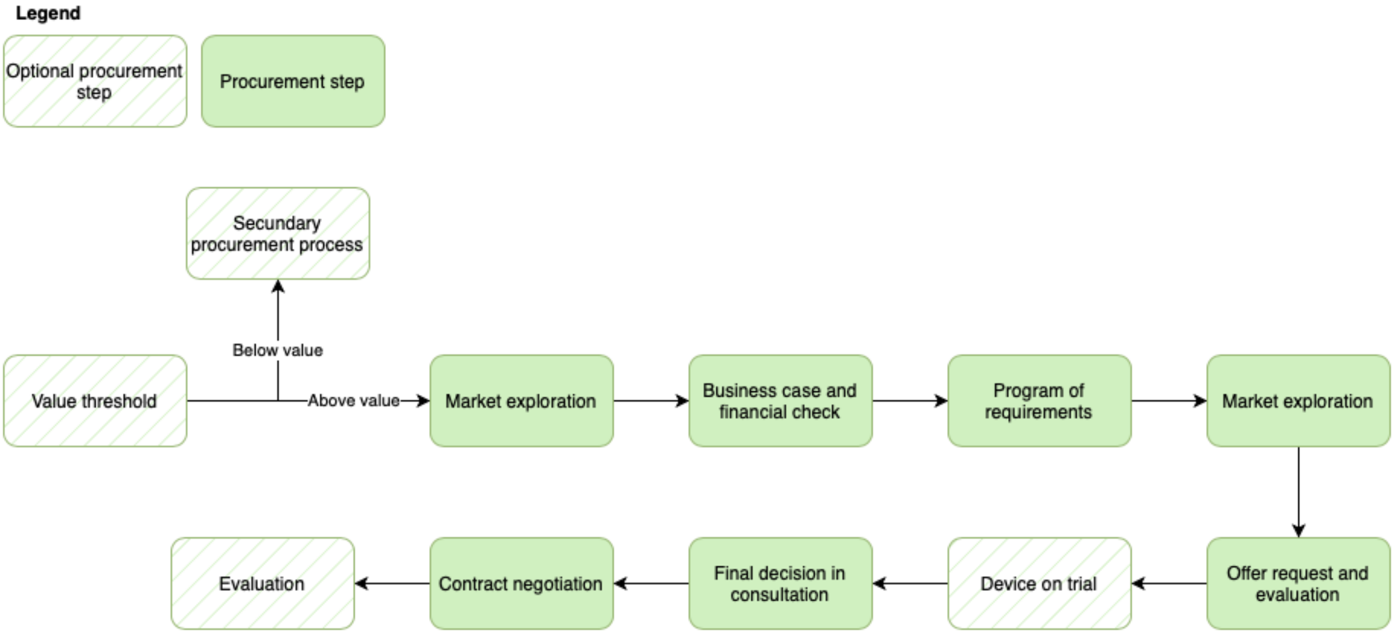


Figure 9 - General overview of the procurement process in hospitals

Hospitals 1 and 2 both have a value threshold, somewhere around a couple of thousand euros. If it is below that value, hospital 2 has a secondary, more informal procurement process. However, with medical devices it is almost always above this threshold. If it is above the threshold of hospital 1, offers need to be requested from multiple suppliers instead of just one, as to be able to compare the offers.

Afterwards, the procurement process starts by an initial market exploration that explores the options that are available, but most importantly serves as an estimation for the costs. This exploration is then used to write up a business case, which besides costs also includes reasoning why the device should be procured and can include some initial requirements. H3.P2 summarised it as follows: *"For new investments, such as [redacted for privacy], there is a separate committee in the hospital. An investment committee. And there you must submit an application stating why you feel this is necessary, and a financial substantiation."*

This business case is then proposed to an investment committee of some sort that is tasked with the allocation of funds within the hospital. They can approve the request or ask for clarifications. Once the request is approved, the program of requirements is finalised, based on the contribution of a variety of stakeholders from within the hospital. For example, the doctors put in functional requirements, the infection prevention specialist puts in cleanability requirements, and the IT department sets the IT requirements. H2.P1 summarises it as follows: *"After the kick-off, the program of requirements is drawn up jointly by the various stakeholders with, on the one hand, technical requirements, sometimes additional requirements for the standards you want it to meet, but certainly also functional requirements from the user of what you expect of the device."*

Once everyone has contributed and the program of requirements is finalised, it is sent to the procurement department that does its own market exploration to identify which suppliers could meet the program of requirements. Afterwards, these suppliers are contacted to fill in the program of requirements and send in an offer. Once these filled in programs of requirements and offers are returned, they are shared with stakeholders that contributed to the program of requirements and everyone evaluates them based on their expertise. Everyone's evaluation is then discussed, which results in a preferred option. Although this process is similar in each hospital, H3.P1 summarised it in one quote*: "So normally that program of requirements is then sent to the possible companies, preferably always more than one (...) who then submit a quotation and with a filled in program of requirements that states: yes, we meet all those requirements and wishes. What options do we have, etc.? After which you can assess the substantive picture and the financial picture."*

When there is still some doubt, a device could be installed on a trial basis, although optional. This is done to gain a better understanding of the device. H3.P1: *"Yes, you often receive it for a week or so, so you can use it, because it is always more difficult to assess it on paper than in real life."* If a device is too large, site visits to other hospitals are planned, H2.P1: *"If it is small equipment, you can often have the equipment brought here. For large equipment, we sometimes go on site visits to other hospitals where the equipment is already installed."*

The final decision on which device to procure is made in consultation with everyone that contributed to the program of requirements. Everyone voices their preferences based on their expert evaluation of the offers, after which these preferences are compared, and a final decision is made. H2.P1*: "And then you actually make a joint choice based on financial, technical from our department, also in terms of maintenance and serviceability, and from a user perspective you get an assessment, so to speak. And then you come together and as a project group you decide, okay, we'll go left, we'll choose manufacturer A with that device or manufacturer B with that device."* In addition, several participants mentioned that if there isn't a joint preferred option because multiple devices would suffice, that the end user can make the final call based on their preference. H3.P1: *"But the main point is more if there is no veto from departments such as medical technology or ICT, then it really is still mainly down to the functional choice of the user."*

Finally, the procurement department starts contract negotiations with the preferred suppliers in which the final price and aftersales are discussed. Once an agreement is made, the devices can be delivered and installed. This also allows for potential evaluations of the procurement process, the supplier, and the contract, especially when the procurement process did not go smoothly. H2.P1: *"Sometimes you have an evaluation of the purchasing process, if there are reasons for it. If things have gone very smoothly or things haven't gone well."* In addition, the services of the manufacturer are continuously monitored, H1.P1*: "[The contract] is then evaluated and then looked at, is that okay? How is the supplier performing compared to the agreements? This is then actively managed. If, well, it's good, we don't have to act on it, but if things go wrong, we will send it to the supplier and an improvement plan will be set up."*

During the procurement processes within the hospitals, there is a dynamic between a 'project group' that is actively involved in the process and a supervisory group that supervises the process and allocates funds. The hospitals phrase this differently, but the concept remains the same. For example, at H1 the supervisory group is called the steering committee, whilst at H2 and H3 it is called the investment committee. Both the project and the supervisory group can consist of multiple different stakeholders from within the hospital and are different per hospital. This is shown in Figure 10 below.

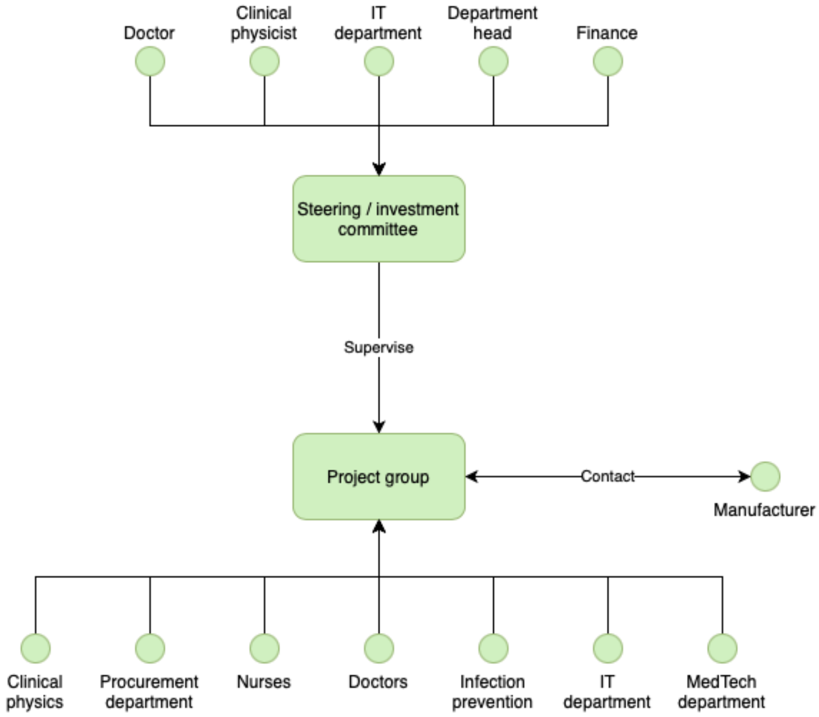


Figure 10 - Supervision during the procurement process in hospitals

Besides the general process of procurement, participants also mentioned several other interesting notions, of which three focused on the dynamic between the different stakeholders involved during the process. The first is that there is a clear division of roles between the different stakeholders. For example, H1.P2 mentioned: *"(...) we had an explicit ban on talking about money and committing to [a supplier]."* This division of responsibility can also lead to unpleasant results, as H2.P1 recalls: *"(...) you buy a device that also includes a piece of software and then we installed it as medical technology department. It was technically completely in order, but in the end the user was very unhappy, because the software had not yet been checked and rolled out and did not work at all."* This happened because the medical technology department and the IT department did not actively communicate during the procurement process and the instalment. This has resulted of the merger of the two departments in H2, but it symbolises how all stakeholders involved during the procurement process can very much be only focussed on their own expertise and everyone has their own very specific role from which they contribute to the process.

Second, participants called the procurement process complex due to the large number of stakeholders involved and the many different steps that must be taken. This could sometimes lead to some friction during the process. Yet, this has always been overcome so it was never a big issue. As an example, H2.P1 mentioned: *"For example, we recently had a project in which my department is subdivided into different domains with technicians. We have 4 domains, and each domain actually manages its own type of equipment, so to speak, but sometimes you have procurement processes, which cross domains even within our own department, so the technicians from those different domains must also work together to arrive at one good solution."*

Third, participants from both H2 and H3 both mention some discrepancies between the different stakeholders involved in the procurement process. This is most noticeable in the wishes, or requirements, that each stakeholder sets for the new device. In the context of cybersecurity, this can result in requirements set by the IT department, for example the use of multi-factor authentication, but for the doctors this takes up too much time, which they do not have. This discrepancy can sometimes lead to small disputes between the involved stakeholders but is usually resolved. As an example, H3.P1 mentioned: *"We actually have, but that is still a difficult process, standard requirements for ICT that things must meet. (...) The IT department wrote this in a very IT-minded manner. And a software package or a medical device is not the same thing. And we are really confronted with the fact that they demand, for example, they say: yes, all software must be able to run on our virtual servers. You know? These are the standard requirements for software packages. But that doesn't work for medical devices."*

Finally, hospitals might actively collaborate with other hospitals during the procurement process for various reasons. Only H2 mentioned that they do not actively collaborate with other hospitals during the procurement of new medical devices. They do, however, collaborate on more general procurement processes such as HR tools, H2.P2*: "There is often collaboration with other hospitals or joint purchasing for hospital-wide matters. I don't see it that much for medical equipment."* The other two hospitals do collaborate on the procurement of medical devices. They both do this in order to drive down costs by buying larger quantities at once. H3 also mentioned that they procure certain devices or software together with other hospitals to make the exchange of patients easier between hospitals. When a patient is admitted to one hospital but has to receive specialised treatment from another hospital, it is easier if the medical devices, specifically imaging equipment, is shared. H3.P2 mentioned: *"They refer patients to us who are actually eligible for a certain treatment. And [procuring the same] software also makes it possible for us to quickly view the data of patients who are referred to us. Because these are treatments that simply have to be done right away."*

4.3.4 Requirements

All participants were asked what requirements are typically set during the procurement process of medical devices. This resulted in 11 requirements mentioned during the interviews: aftersales, cleanability, compatibility with other systems, cybersecurity, data security, price, regulation compliance, reliability, repairability, safety, and supplier satisfaction. All these requirements were considered by all participating hospitals.

A lot of the requirements set during the procurement process are functional, such as aftersales, price, regulation compliance, reliability, repairability, and safety. Aftersales is concerned with the services suppliers offer to hospitals after the device has been installed. For example, training and instructions for the users, but also repair services, H1.P2: *"In the procurement process it is A) about the purchase price, B) about the requirements plan, and C) also about aftersales. You know, if the pump breaks on Sunday morning, what's the service of having someone [to fix it] next to you within an hour?"* This is crucial when the medical technology department of the hospital cannot repair it themselves. Therefore, this is closely related to two other requirements: reliability, and repairability. Reliability focusses on the continued operation of a device without any downtime, but also on the quality of the devices themselves. H2.P1 mentioned this as follows: *"We from medical technology provide an opinion on which is the best choice from a technical* *point of view, on the one hand regarding the device itself, but on the other hand also with regard to the maintenance proposals that come with it."* Repairability, on the other hand, is concerned with if the medical technology department of the hospital is capable of repairing the device themselves, and if spare parts are readily available. H1.P2 mentioned: *"The instrumental service of a hospital solves common problems, so they also want to look at the device. If it breaks, can you do a lot yourself and do you have a lot of spare parts? So spare parts, how many do you need?"*. If the hospital is not capable of repairing the device themselves, then aftersales becomes important, because the manufacturer will need to come and solve the problem.

Safety and regulation compliance are somewhat related. The clinical physicists are tasked with evaluating the safety of the devices, especially when radiation is involved, H1.P1: *"Clinical physics colleagues check whether the standards and certifications are all being met. For example, whether it is all done safely when it comes to radiation in radiology, right?"* Although part of this evaluation is to verify whether the devices meet the right safety standards, regulation compliance goes further than that and also encompasses more general device regulations, such as the MDR. Again, H1.P1 mentioned it as follows: *"It is checked whether they meet the correct CE or NEN certification, or the ISO if that were allowed, or the MDR, you know, all those types of certifications. And they will also be asked to show that certificate."* In addition, H3.P1 mentioned that hospitals are required by law to verify the compliance with relevant regulations: *"(...) we must ensure that the devices we purchase have proper certification. So, we have to check that too."*

Of course, the price of the device is also important to consider. As mentioned in the previous section, before offers are requested from suppliers, funds are allocated to the procurement of the new devices. Therefore, there is set maximum budget that can be spend during the procurement process. H3.P2 even mentioned that costs can be the most important consideration during the procurement process: *"But in hospitals, I think cost is always the most important consideration."*

Supplier satisfaction is also considered during the procurement process, mostly in the negative way. When the hospital has had a negative experience with a supplier in the past, this might persuade them to opt for a different supplier during the procurement process. H2.P1: *"Yes, that is actually reflected in that technical assessment, so if we simply have bad experiences with suppliers from our department and we can substantiate that, then we would also like to include that in our technical advice. (...) the user also benefits from the fact that no matter how beautiful a device is, it also benefits from the moment that you experience problems and malfunctions that occur, that it is handled in a fluid manner by my department and by the suppliers. (...) if we say: that party is not reliable, does not deliver, is not available, etc., then that is definitely a heavy weighting factor, why a supplier should not be chosen."*

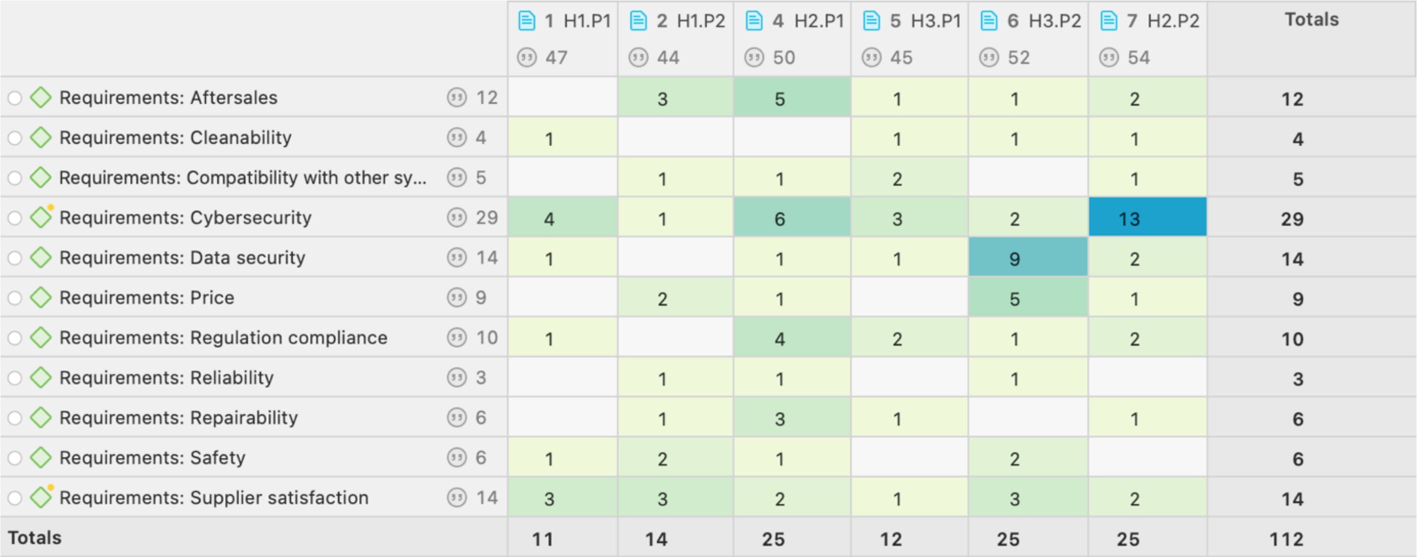
However, besides these more functional requirements, there are also requirements set that are IT related, such as compatibility with other systems, cybersecurity and data security. Compatibility with other systems is a broad requirement that can encompass IT systems as well as other physical systems. For example, H2.P2 mentioned that a device should be able to work with a bedsore device in an operating room: *"(...) we have the device, but it has to work together with, for example, a fluoroscopic examination device with an operating room table. Well, that should be able to revolve around each other well."* Additionally, devices should be compatible with the already existing IT systems within a hospital, such as the hospital's network and electronic patient file system. H1.P2 mentioned this: *"You have an electronic patient file; it contains electrical hubs and then you click the device into it. However, your electronic patient file should be able to understand this."*

When it comes to the cybersecurity of medical devices, it can be concluded from the interviews that hospitals prefer it if the devices are placed within their own isolated network segment within the hospital and that there is no communication with external networks. This is also evident in the requirement all hospitals set that obliges manufacturers to disclose how their device works and communicates, so that the hospitals know how to integrate it within their network and understand which data is transmitted where. Devices should also be compatible with the cybersecurity measures that are already in place on the hospital's network. Additionally, software updates and security patches are also discussed with the manufacturer and are a part of the contract negotiations discussed in the previous section. Yet, from all the different interviews it can be concluded that hospitals do not prioritise cybersecurity over other requirements that are set. Contrary to this, they often rely on making sure the devices are cybersecure after they have been procured. For example, by making sure they only operate within their own segmented, safe network. H2.P2 summarises it as follows: *"But actually [cybersecurity is ensured] by the strict requirements, the strict network requirements. Cybersecurity actually means that you want to prevent people from outside getting into your system. But we have already set it up in such a way that it runs in a bubble that it does not come out at all."* This shows how hospitals prefer to rely on the cybersecurity they add afterwards, instead of on the cybersecurity that comes with the medical device. This allows them to not prioritise cybersecurity over other, more functional requirements.

Besides cybersecurity, all hospitals also consider data security. Most participants mentioned this in relation to data being processed by a third-party. For example, H1.P1 mentioned: *"Many hospitals set the requirement, or at least we set the requirement, that when we work with a SaaS solution, that our data stays within Europe."* H3.P2 goes a step further with stating that data should not leave the hospital, even when third-party software is used: *"(...) the requirement from the hospital is that they look particularly closely at how it is guaranteed that the data actually stays within the walls of our hospital."* In part, these requirements are set to comply with the GDPR.

Table 11 below is an output from ATLAS.ti that depicts how often each requirement was mentioned during the interviews.

Table 11 - Code distribution per requirement



		1 H1.P1 47	2 H1.P2 44	4 H2.P1 50	5 H3.P1 45	6 H3.P2 52	7 H2.P2 54	Totals
Requirements: Aftersales	12		3	5	1	1	2	12
Requirements: Cleanability	4	1			1	1	1	4
Requirements: Compatibility with other sy...	5		1	1	2		1	5
Requirements: Cybersecurity	29	4	1	6	3	2	13	29
Requirements: Data security	14	1		1	1	9	2	14
Requirements: Price	9		2	1		5	1	9
Requirements: Regulation compliance	10	1		4	2	1	2	10
Requirements: Reliability	3		1	1		1		3
Requirements: Repairability	6		1	3	1		1	6
Requirements: Safety	6	1	2	1		2		6
Requirements: Supplier satisfaction	14	3	3	2	1	3	2	14
Totals		11	14	25	12	25	25	112

The frequency of mention can be an indication of the importance of each requirement during the procurement process. In that case, the importance of the requirements during the procurement process would be as follows:

Table 12 - Requirement importance based on frequency of mention

Position	*Requirement*	*Frequency of mention*
1	Cybersecurity	29
2	Data security	14
2	Supplier satisfaction	14
3	Aftersales	12
4	Regulation compliance	10
5	Price	9
6	Repairability	6
6	Safety	6
7	Compatibility with other systems	5
8	Cleanability	4
9	Reliability	3

From Table 12 above it can be concluded that cybersecurity and data security would be the most important considerations during the procurement process. However, these results are skewed, as during the interviews more time was spent on inquiring about cybersecurity, which results in it being mentioned more often. Therefore, a sound conclusion for the importance of requirements cannot be made based on these results.

This is backed up by several quotes from participants when they were asked how better cybersecurity of one device over another might be weighed during the procurement process. H2.P1 said: *"(...) it must meet [cybersecurity requirements]. That is the starting point. So, it must comply. But it doesn't really matter if something is extra safe or extra well protected."* H1.P1: *"Cybersecurity is not necessarily specifically prioritized. But it is simply included as a minimum requirement and if it does not meet that requirement, then we simply do not buy it, period."*

In addition, H3.P2 mentioned that the price might be the most important consideration*: "But in hospitals, I think cost is always the most important consideration."* Also, in the previous section it was discussed that the final decision is always made in consultation with all stakeholders that contributed to the procurement process. Even though this is the case, several participants mentioned that the final decision is often influenced by the preference of the end-user. H3.P1: *"(...) the main point is more if there is no veto from departments such as medical technology or ICT, then it really is still mainly down to the functional choice of the user."* Or, H2.P2 mentioned: *"So it is usually during the final decision that everyone says: okay, we all support choice x or y and sometimes the department itself or the doctors also decide yes, but I really want that device."* Therefore, what is deemed most important can change every time based on the preference of the end-user for the specific device that is being procured.

In conclusion, what requirement is deemed most important can differ per procurement process and the end-user that is involved. Based on the data of this thesis no sound conclusion can be drawn on what requirement is considered to be most important across several procurement processes.

4.3.5 Regulations

Participants mentioned several different regulations they follow during the procurement process, or that manufacturers need to follow. Most regulations mentioned during the interviews have already been mentioned in Chapter 3 of this thesis. All regulations mentioned during the interviews were: (1) Convenant medische technologie; (2) the GDPR; (3) the MDR; (4) Regulations set by the medical specialists association; (5) the NEN7510 norm; (6) Tendering law; and (7) Regulations set by the NZa.

Participants from H2 and H3 mentioned that they structure their procurement process according to the 'convenant medische technologie'. This means that their procurement process is documented and structured in accordance with the guidelines set out by that document. The same participants also mentioned that they consider the GDPR during the procurement process. When data and software are part of the device being procured, hospitals verify whether the device complies with the GDPR. H3.P1 mentioned it as follows: "(…) *with equipment where patient data and software also play a major role, you also have to comply with the GDPR. You also have to take this into account during the process."*

All hospitals mentioned the MDR as something they consider during the procurement process. Devices that are being procured must comply with the MDR, and hospitals actively check during the procurement process whether this is the case. H3.P1 mentioned: "(…) *we must ensure that the equipment we purchase has proper certification. So, we have to check that too [during the procurement process].*

H1 and H2 mentioned that they follow the NEN7510 norm. As discussed, in Chapter 3 previously, this has some implications for the procurement process. One of these implications is that the device that is procured also needs to comply with this norm. These requirements can be set by the IT department of a hospital, H2.P1: "*ICT is of course putting pressure on NEN7510, to ensure that we comply with it."* Participants from H3 did not mention the NEN7510 norm, although it is likely that they still adhere to this standard, as it is good practice to do so.

What was not discussed previously in Chapter 3 were guidelines set by the NZa and the medical specialist association. Participants from both H1 and H3 mentioned that these guidelines might be the reason to start a new procurement process and may influence the requirements set for the new device. H3.P2 mentioned it as follows: "*They draw up a set of requirements stating what a hospital must meet to treat certain [redacted for privacy]. And that includes software, but also what qualities and competencies the [doctors] must have for this*." The publication of these guidelines might also be the reason to start a new procurement process and motivate why funds need to be allocated to procure this new device, H3.P1: "*These are guidelines and advice and are used by the department as motivation [for the new procurement process]. So, they refer back to it (...)."*

Finally, H1.P1 mentioned that all non-academic hospitals do not have to comply with EU tendering law. This means that they do not have to put out a public tender when they procure new devices.

For an elaboration on the implications of all the different regulations, please look back at Chapter 3.

4.3.6 Other

In addition to the main themes, participants identified several noteworthy observations that did not align with any of the primary themes. These observations were (1) that a procurement process does not always lead to a new device being procured; (2) that participants felt like cybersecurity is not always a priority; and (3) that they noticed a shift towards connected medical devices. The observations were found during interviews with participants from H1 and H2. During interviews with participants from H3 no additional observations were found.

H1.P1 mentioned that not all procurement processes lead to a device being procured: "*(...) We found out during the tender process that the market is not yet mature enough, or the technology is not yet mature enough, to really meet our requirements. So, then we just put that on hold.*" They might restart this procurement process in a couple of years, to see whether the market has matured enough to procure the device. This is often found out during the offer request and evaluation phase, after which the procurement process might be stopped.

For the second observation, participants from both H1 and H2 mentioned that only relatively recently they noticed a bigger cybersecurity awareness. H1.P2, although not a cybersecurity expert, actively questioned how secure the data sharing is with other hospitals when, for example, a second opinion is requested.

Finally, both H1 and H2 participants mentioned that they notice a shift toward more and more connected medical devices being installed at their hospital. H1.P1 estimates that at the moment the share of connected medical devices is around 50% at the hospital. In the case of H2, the IT and MedTech departments merged, as they noticed that they increasingly had to work together due to increase of IT in medical devices. H2.P1 mentioned: "*It used to be that if there was a UTP cable attached [to the device], it was one-way traffic, so you collect some data using a device and then we push that data away in the IT environment and done. And now they are more and more integral solutions, so with software that talks back to those devices, it's a two-way street, there are data streams in there.*"

4.4 Answering sub question 2

This section will answer SQ2: *What are the existing general procurement practices for medical devices in hospitals in The Netherlands?* In addition, the findings from this chapter will be related to work by other researchers.

The procurement practices for medical devices in non-academic hospitals are defined by a complex process that involves many different stakeholders from within the hospital and outside. The hospitals within the sample of this study, even though they were not affiliates and were spread across the country, all had similar procurement processes. This general process is depicted in section 4.3.3, Figure 9 - General overview of the procurement process in hospitals. The steps all hospitals follow are: (1) Market exploration, (2) Business case and financial check, (3) Program of requirements, (4) Market exploration, (5) Offer request and evaluation, (6) Final decision in consultation, (7) Contract negotiation. Besides these steps, optional steps can be taken, such as having the device on trial, or evaluating the procurement process.

This process can be initiated for several different reasons. However, the end-of-life of a current device, or the development of a new technology or treatment are most common. Another more common reason to initiate a procurement process is the release of new guidelines set by the NZa and medical specialists association. They can set new guidelines that if a hospital wants to offer a certain procedure, that their devices need to have certain functions. If the current devices of a hospital do not have these functions, a new device should be procured.

What must be noted is that during the procurement process, a lot of different stakeholders from within the hospital contribute to the procurement process based on their expertise. So, for example, a clinical physicist sets and evaluates radiation safety requirements for a CT scanner. Most stakeholders contribute by setting requirements and evaluating how different offers from manufacturers score on these requirements. However, because everyone is mostly focussed on their own expertise and set of requirements, some discrepancies may occur during the process. For example, the requirements set by one stakeholder clashes with the requirements of another. Yet, these discrepancies are always solved, as the final decision is made in consultation with all the different stakeholders. During this decision-making process, the views of the end-users are always considered, as they are the ones that need to work with the device.

Several regulations are followed during the procurement process. However, they are mostly focussed on the medial device themselves, instead of on the procurement process. Therefore, they do not shape the procurement process beyond the fact that hospitals need to check whether the devices they procure adhere to the relevant regulations.

To conclude, the procurement practices in the different hospitals are strikingly similar and are defined as a complex process to which a lot of different internal and external stakeholder contribute.

4.4.1 Related work

Several other theses and articles have also studied the procurement process of hospitals in the Netherlands. These will be briefly discussed below.

Muittari (2023) researched the purchasing process of high-tech medical devices in the Netherlands. That thesis also mentioned the striking resemblance between the procurement processes in different hospitals. However, as Muittari (2023) researched both academic and non-academic hospitals, the process defined is more general, as academic hospitals have to follow tendering law. The process defined in this thesis is: (1) Problem or need recognition, (2) Information search, (3) Evaluation and negotiation, and (4) Purchasing and using. Although these steps are more general, they overlap with the procurement steps identified in this thesis. Yet, this thesis elaborates on these general steps in the context of non-academic hospitals.

Carrera et al. (2015) researched the cooperative purchasing of pacemakers in the Netherlands. They identified the main reason to collaborate with other hospitals during the procurement process is to drive down costs. In the case of pacemakers, this could result in a price reduction of up to 34%. This aligns with the reason for collaboration found in this thesis. However, Carrera et al. (2015) also identified the learning possibilities for the procurement department as a reason to collaborate. By collaborating with other hospitals, procurement departments can learn from each other and improve efficiency. This thesis adds another reason to collaborate on the procurement process: to streamline the devices between hospitals to enhance patient transfers between hospitals.

Minning (2020) studied the reputation of medical device manufacturers and how this might influence the procurement department in a hospital. That thesis identified that the reputation of a manufacturer can influence the advocacy and purchasing decision of the procurement department. Manufacturer reputation is influenced by multiple different factors such as, services, safety, customer focus, and their products. This aligns with the sub-code ‘supplier satisfaction’ discussed in this thesis.

Finally, Salm (2022) identified challenges in the decision-making process of Dutch hospitals in the context of the procurement department. That thesis found that the complex nature of the procurement process and the hospital as an organisation resulted in a clear structure and division of roles. This was also evident in the description of the procurement process in this thesis.

5 External influences on the procurement process

This section will focus on analysing the influence and view of stakeholders outside of the procurement process in hospitals. In doing so, it will answer SQ3: *What is the effect of external stakeholders on the procurement process of medical devices in the context of cybersecurity?*

5.1 Participant population

As specific participants knowledgeable on the topic were approached for this study, the sampling was purposive (Bryman, 2016). As mentioned previously, this can be distinguished in the sampling of context and the sampling of participants.

In terms of the context, a broad sample was set. All organisations that are knowledgeable either on cybersecurity or healthcare regulations were considered. This way a broad array of potential outside influences and stakeholders could be considered in this study. Participants were sampled based on their knowledge on hospitals. This means that they should be knowledgeable about hospitals in the context of their professional background. For example, this means that a cybersecurity specialist should have knowledge on cybersecurity in hospitals and that a policy professional should be knowledgeable about policies for hospitals, and not general practitioners or physical therapists. This to ensure that their knowledge and view is specified to hospitals and not just the healthcare sector.

Several organisations were contacted for their willingness to participate in this study. However, only one organisation responded. This resulted in one interview conducted with two participants which lasted for 26:12 minutes. Participants were asked about their experiences with cybersecurity in hospitals, and specifically their experiences with the procurement process. For example, whether they are often involved in the process or if they have any official advice for hospitals to follow during the procurement process. The interview protocol used during this interview can be found in Appendix A.2. Participants were also asked about their experience with this topic at their current organisation. An overview of the participants can be found in Table 13 below.

Table 13 - External stakeholders interviewed

Ex. Org. ID	*Participant ID*	*Combined ID*	*Role*	*Experience*
1	1	E1.P1	Cybersecurity specialist	7 years
1	2	E1.P2	Cybersecurity specialist	1.5 years

5.2 Thematic analysis

Because only one organisation is interviewed here, a framework analysis is not well suited as there is no comparison between different organisations. However, the first two steps of the framework analysis, (1) data familiarisation and (2) identifying a thematic framework, essentially form the basis of a theme analysis (Bryman, 2016). Therefore, these same two steps were followed to identify major themes in the interview, whilst the other framework analysis steps are not followed. The first step consisted of familiarising with the data at hand and assigning preliminary codes to the data. This resulted in 15 preliminary codes. After a second inspection two codes were merged due to similarity, which resulted in a total of 14 codes, linked to 22 quotes from the interview.

In the second step, the 14 different codes consisting of concrete descriptions were merged into more abstract overall themes. This resulted in three major themes found within the interview. The 14 initial codes remain as sub-codes of these three major themes. These themes are described in Table 14 below.

Table 14 - Thematic analysis of external stakeholders

Theme	*Description*	*# of sub-codes*
Organisational activities	This theme focusses on the activities that E1 performs as an organisation. Specifically, how they help hospitals with their cybersecurity needs and how they are in contact with hospitals.	5
Procurement experiences	Procurement experiences cover all experiences E1 has with the procurement process in hospitals and how they are involved in this process. This also includes things they noticed about the innerworkings of the procurement process.	7

Theme	*Description*	*# of sub-codes*
Sector developments	This theme entails the sector developments the participants notice. Next to this, it includes what they think must be improved cybersecurity wise in the Dutch hospital sector.	2

The codebook of the theme analysis and the framework analysis can be found in Appendix C.

5.3 Discussion

This section will discuss the results from the external stakeholder interview, as well as the framework of the 'outside influences' theme of the hospital interviews. These results are detailed below.

5.3.1 External stakeholders

This section will elaborate on the themes found in the interview with the external stakeholders. Each theme will be discussed and elaborated upon with quotes when necessary. As the interviews were conducted in Dutch, all quotes are translated into English.

<u>Organisational activities</u>

As cybersecurity specialists, the main request they receive is for cybersecurity advice. These requests mostly come from hospital CISO's or other cybersecurity personnel. Sometimes they do have contact with medical personnel, but this happens rarely. The advice they give is centred around threat reports, vulnerability disclosures, or mitigation measures that need to be implemented. Their specific focus thereby lies solely on hospitals. They do have contact with manufacturers, but only when manufacturers warn them about a certain vulnerability. E1.P2 clarifies: "*We do have relationships with some parties when there is a vulnerability in the medical product, that they can share this with us and that we can discuss this with our target group.*" However, it could be that other cybersecurity specialists do combine their advice for both manufacturers and hospitals, but the sample size from this study is too small to conclude that.

In addition to the advice they give on demand, they also proactively check the security of hospitals, for example if data from the hospital is leaked somewhere. If this is the case, they notify hospitals of a potential breach. Lastly, they put different hospitals in contact with each other so that they can share experiences. As an example, E1.P1 mentions: "*These are often discussions that hospitals have with each other, right? How did you deal with this part of the NEN7510? How have you secured this within the organisation?*" This example illustrates how hospitals try to learn from each other's experiences, where cybersecurity specialists can function as a linking pin.

<u>Procurement experiences</u>

When asked whether the cybersecurity specialists had any official advice on the procurement of medical devices the answer was quite simple: no, they do not. However, they are still sometimes involved in the procurement process in hospitals. This is often the case when hospitals procure specific cybersecurity services or software. It is possible that this relates to securing medical devices, but not necessarily. This also relates to a second point made by E1.P1 that sometimes cybersecurity is only considered after procurement has already taken place: "(…) *sometimes you actually have no choices at all and, as a security organization within a hospital, you just have to make do with it, so to speak, and you try to apply measures around that device in order to still somewhat meet the security level that is required.*"

This can be explained by three other themes found in the interview. First, the cybersecurity specialists notice that the views on cybersecurity within hospitals can differ greatly, E1.P1: "*Even if you look within some hospitals, you see that there is a difference there too, right? Because if you ask the CISO, they think it is very important. But if you then ask a specialist doctor, he says yes, but I just need this thing to do my job.*" Second, this is underpinned by the lack of choice hospitals have when selecting medical devices. E1.P1 mentions that even when hospitals choose to prioritise cybersecurity when procuring new medical devices, the chance exists that the devices do not differ that greatly, as they only have a few manufacturers to select from. Finally, the cybersecurity specialists notice a priority within hospitals to offer care as efficiently as possible, where it is challenging to strike a balance between security and efficiency. E1.P1 illustrates: "(…) *If you look at the average nurse or doctor or things like that, they often have one major intrinsic motivation, they just want to help people. That's what it comes down to and everything you do as a security professional often makes it more difficult, so it is very difficult to find a balance in how do we ensure that we are safe, without medical staff feeling inhibited* (…)". These three points currently make it harder to prioritise cybersecurity within the procurement process of new medical devices.

Finally, the cybersecurity specialists did mention one procurement-specific question they get asked sometimes: how to deal with devices from foreign manufacturers. E1.P2 mentions: "(…) *what sometimes comes along is devices from abroad. Do we want Chinese devices in our hospitals, or do we want American devices?"* This exemplifies that hospitals do consider the origins of their supply chain. In part, this could be due to the requirements set out by the NEN7510 norm, as discussed in chapter 3.4.1. This norm requires hospitals that contracts should incorporate requirements for information security risks in the supply chain of IT services and products. However, it is unclear from this quote whether these hospitals do follow the NEN7510 norm.

Sector developments

The cybersecurity specialists noticed one major shift within the sector, but still see room for improvement. They notice that manufacturers are becoming more and more aware of their responsibility to deliver cybersecure devices, albeit due to more stringent regulations such as the NIS2 and MDR. In their opinion, this has resulted in more cybersecure devices recently. It even motivates some manufacturers to install an extra device on the hospital's network to remotely update their devices. However, where this motivation comes from is not clear, E1.P2 mentions: "*I think this may also have to do with regulations, that the manufacturer may be held responsible, but I don't know exactly how this works*." However, although these are good developments, they do mention that this development is still slow due to stringent safety regulations posed on manufacturers. E1.P1 elaborates: "(…) *that [development] is still very slow and of course that also has to do with a lot of safety regulations that they have to comply with, right? I think, if you have a large medical device and you want to change something about it, then in America, for example, you have to go through all the FDA hoops to get that device approved again in order to be allowed to put it on the market. So, quickly patching or adjusting something because it is more secure, that just doesn't happen*." They blame this on the dilemma between security and safety, where additional steps to smooth out the process of patching should be taken.

Second, the cybersecurity specialists mention that in order to improve cybersecurity within hospitals, education is the key. By educating staff on the importance of cybersecurity within the organisation and explaining why certain cybersecurity measures were implemented, basic cyber hygiene practices can be improved. In the end, this might even result in cybersecurity becoming a bigger priority during the procurement process, when more stakeholders agree on its importance.

5.3.2 Outside influences

During the interviews with hospital stakeholders, several influences from outside of the hospital were discussed. These influences were specific on the procurement process itself of medical devices. Therefore, regulations and regulatory bodies are not considered in this section, as these might influence how the process takes shape, but do not exert any extra influence during the process itself. For example, tendering law shapes the way academic hospitals should procure new medical devices prior to the start of the process but does not exert any extra influence when the process is taking place.

All hospitals mentioned the influence of manufacturers during the procurement process. Manufacturers might be actively involved during the procurement process through various ways. First, H1.P2, as part of the medical staff, recalled that he was actively contacted by manufacturers during the procurement process: *"There was a very large tender for ventilators and then I was personally called by suppliers. Like: 'We feel that we are going to miss that order. What is going on?'"* This whilst, also discussed in section 4.3.3, the procurement department of hospitals often are the contact person for manufacturers. Doing this, manufacturers might actively try to influence the procurement process for their benefit. In addition, there is direct contact with the manufacturer for additional question and the possibility to have the device on trial. For example, H3.P1 mentioned questions to the manufacturers such as: *"Well, that is, for example, about the functional possibilities, whether or not they can explain it better or if you as a user say: 'But can I do this with it or not? Or how does this work?'"* This participant also mentioned the possibility to use devices on trial: *"With some devices you also do trial installations. These are always supervised by the manufacturer involved. They often just come along. So, then they also come into the hospital."*

Manufacturers might also try to sell their devices by visiting medical conferences. H1.P2 recalls visiting such a medical conference: *"At conferences [the manufacturers] all have stands and such. Then you walk past there, and you know that seller, they know you. 'Hey H1.P2, we have something new, come take a look man.' Well then, they show the new devices and this and that is useful and all that. 'Gosh, shall we come by sometime, so we can chat some more?'"* Participants from other hospitals did not mention medical conferences.

These medical conferences also facilitated another outside influence: that of other doctors. Doctors amongst each other might boast about their shiny new device they just got. H1.P2 would even describe it as macho culture: "*And as doctors amongst yourselves, (...) it was kind of a macho thing. 'What new device do you have? Oh, you don't have anything new? I'll pay for dessert then.*'" However, doctors will also share their experiences with devices in a more friendly way. For example, by sharing how they like the new device they just got and how it may help others. H2.P2 mentioned: *"Sometimes visits are made to other hospitals to see how the product is liked there."*

5.3.3 Stakeholder analysis

Figure 11 expands the internal stakeholder analysis from section 4.3.1 to also include the stakeholders from outside of the hospital. This figure visualizes the dynamics as discussed previously in this chapter.

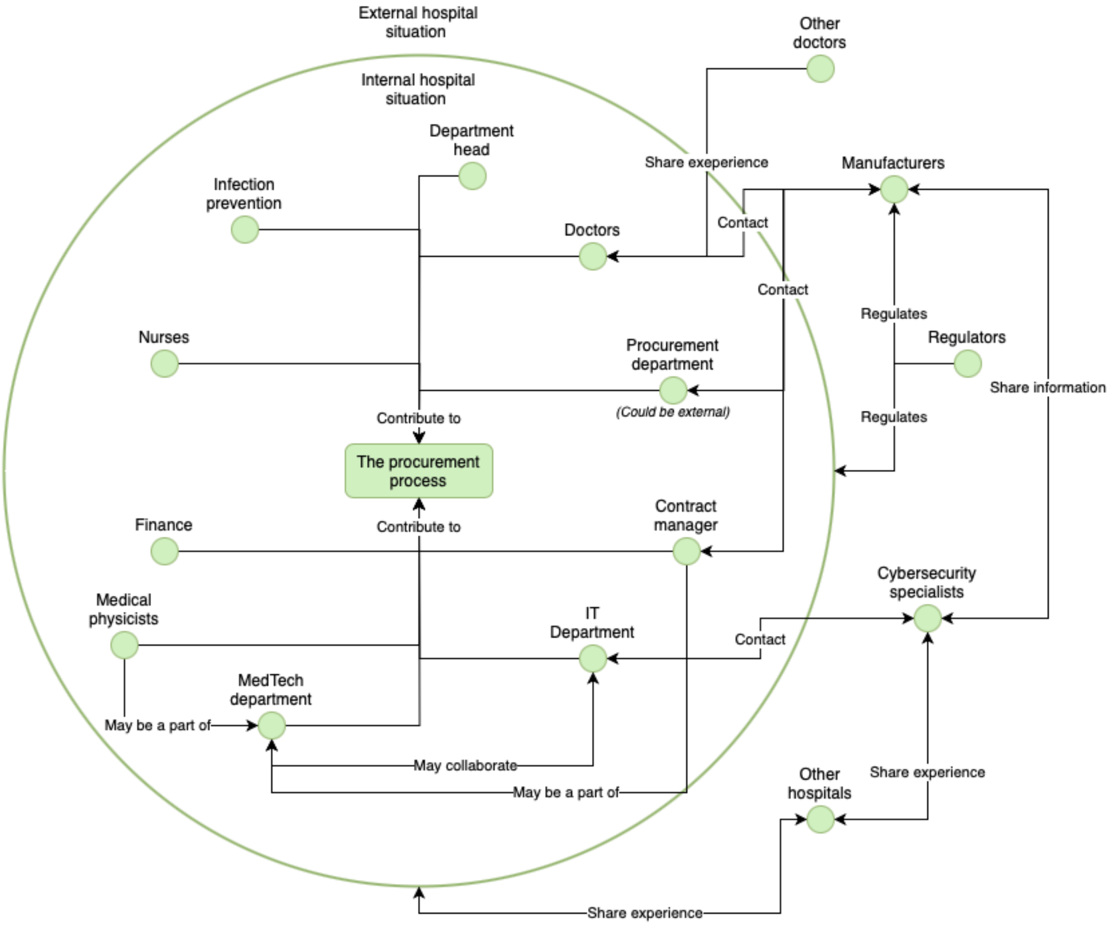


Figure 11 - Expanded stakeholder analysis

Besides the stakeholder analysis provided above, a power-interest grid of the external stakeholders is presented in Figure 12 below. A power-interest grid has two dimensions: power and interest (Ackermann & Eden, 2011). Interest shows the stakeholder's interest in the issue at hand, whilst power depicts the stakeholder's power to affect the issue in the future (Bryson, 2007). In the case of this thesis, the issue at hand is the cybersecurity of medical devices. Five stakeholder groups are shown in this grid: manufacturers, regulators, hospitals, cybersecurity specialists, and other hospitals and doctors. This power-interest grid was not used for the internal stakeholder analysis, as one of the key take-aways from the previous chapter is that the procurement decisions are made in consultation with all involved stakeholders. Therefore, a consensus is achieved where everyone's voice is considered equally, which diminishes the added value of a power-interest grid.

First, manufacturers in theory have all the power, as they are the ones that design the medical devices and thereby can implement the cybersecurity features they desire. Additionally, E1.P2 notices a shift in the sector that manufacturers become more willing to implement these cybersecurity features. However, as mentioned in the introductions of this thesis, Lam & Wong (2018) notice that the willingness to add these features can differ greatly per manufacturer. Therefore, the interest for manufacturers to implement these cybersecurity features is deemed medium-low.

Second, regulators currently show a medium interest in the cybersecurity of medical devices, with some regulations that provide minimum requirements. Yet, the way they shape these requirements make them less powerful than the manufacturers themselves, As can be concluded from chapter 3, a lot of the regulations are based around risk analyses that manufacturers themselves conduct. So, whilst regulators do have the power to not admit a certain device onto the market, they do not fully exert this power to set stringent minimum requirements. Therefore, their power is medium high.

Third, from the interview conducted for this thesis it can be concluded that mostly IT departments and their CISO are concerned with cybersecurity of medical devices, whilst other stakeholders involved in the process are less aware of the importance. Therefore, the interest for hospitals is medium high, as it is considered important, but not by all stakeholders. On the other hand, hospitals do have the power to choose more cybersecure devices during the procurement process. However, as E1.P1 mentioned during the interviews, hospitals often have a lack of options to choose from. This therefore limits their power to choose the device that they want, as other factors such as costs also have to play a role.

Fourth, cybersecurity specialists show a huge interest in making sure that hospitals can operate in a safe manner. This was also apparent during the interview. However, as they only have an advisory role, they have little power over the procurement process itself.

Finally, from all interviews conducted for this thesis it can be concluded that hospitals and doctors show a legitimate interest in helping each other and learning from each other's experiences, albeit that their own hospital remains the top priority of course. Therefore, their interest is medium. Additionally, their power over the process is low, as it is only based on sharing experiences.

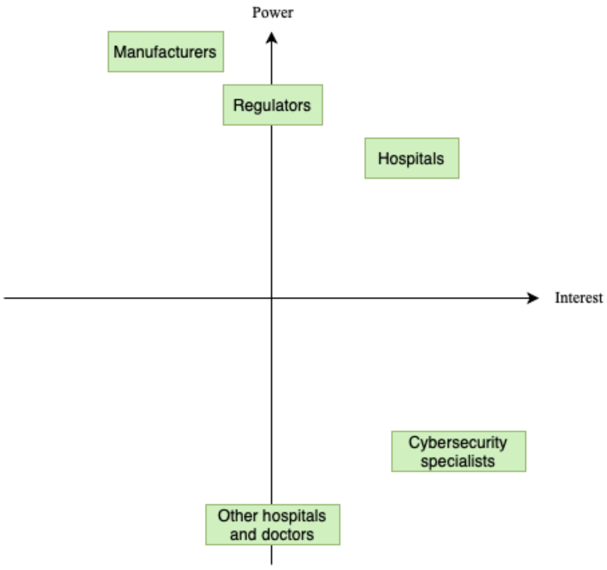


Figure 12 - Power-interest grid of the external stakeholders

5.4 Answering sub question 3

This section will answer SQ3: *What is the effect of external stakeholders on the procurement process of medical devices in the context of cybersecurity?* Additionally, these findings will be related to work by another researcher.

The role and influence of external stakeholders during the procurement process should not be dismissed. First, different hospitals and doctors will actively share their experience with each other regarding a certain device or procurement process. From the interviews it can be concluded that this input is considered during the procurement process and not dismissed, which thereby could influence the final decision.

Additionally, manufacturers play a big role during the process. This role goes beyond the standard preparation of a quotation, as manufacturers may try to actively sell their product to the hospitals throughout the procurement process. This can take shape as a trial period for their device, so that the hospital can already try the product out before deciding on their purchase. However, in some cases, manufacturers might even forego the procurement department of a hospital by consulting with doctors what might persuade the hospital to choose them as a supplier. Although doctors are instructed to not act on this, it does show the persuasiveness of manufacturers during the procurement process.

Next to this, the exact influence of regulations and regulatory bodies on the procurement process remains uncertain. Although they do have a significant effect on shaping the procurement process for academic hospitals through tendering law, this does not apply to non-academic hospitals. However, the NIS2 directive does impose some requirements for cybersecurity considerations during the procurement process, but this has yet to be transposed in Dutch law, so the exact effect remains unclear. Regulatory bodies do however already have some influence on the minimum cybersecurity requirements for medical devices.

Finally, cybersecurity specialists only play a minor role during the procurement process of medical devices. Even though cybersecurity is considered during the procurement process, this is often assessed by the hospital itself and not the external cybersecurity specialists. They do play a role in procurement processes of more cybersecurity related issues, such as the procurement process of anti-virus software. Next to this, they can serve as a linking pin for hospitals to share their experiences with cybersecurity related matters. However, their role during the specific process of procuring medical devices can be deemed small.

To conclude, the different external stakeholders discussed during the interviews all have a different influence on the procurement itself. Of these stakeholders, the manufacturers might have the biggest influence, as they will actively try to sell their product. Furthermore, other hospitals and doctors might influence the process by sharing their experience with a certain device or process. Regulatory bodies and cybersecurity specialists play a minor role during the procurement process, although this might change when NIS2 is transposed into Dutch law.

5.4.1 Related work

Salm (2022) studied the relationship between a doctor and the manufacturer and how this might influence the procurement process. It used to be that this relationship could dictate the device being procured. However, since hospitals have become more complex and the procurement processes more structured, this is not the case anymore. Still, this relationship can influence the procurement process, albeit to a lesser extent. This also aligns with this thesis, as this thesis found that although these relations still exist, doctors may not discuss the procurement process with the manufacturer.

6 The role of cybersecurity during the procurement process

This chapter will focus on explaining the role of cybersecurity during the procurement process compared to other requirements. To do this, first a theoretical lens is proposed to compare the different requirements. Afterwards, this lens is applied to the requirements and reasons for procurement initiation discussed in sections 4.3.4 and 4.3.2 respectively. Finally, an answer will be given to SQ4: *How are cybersecurity aspects considered compared to other considerations during the procurement of new medical devices?*

6.1 Theoretical background for analysis

To define and explain the role of cybersecurity during the procurement process of medical devices, a theory search was performed. Here, theories that could explain the complex nature of the process were considered. However, not one theory was deemed suitable enough to explain the role of cybersecurity during the procurement process, as the focus of the theories considered was not broad enough to encompass the complexity of the procurement process or technology switching behaviour. Therefore, a combined approach of the push-pull-mooring theory and the complex decision-making framework is synthesised. First, the two will be discussed separately, after which a combined approach is detailed.

6.1.1 Push-Pull-Mooring

The Push-Pull-Mooring (PPM) theory has its origin in migration literature to help explain human cultural and geographical movements (Moon, 1995). Later, the theory has also been applied to explain switching behaviour or intention towards adopting new technologies (Lenz et al., 2023). Therefore, it is linked to similar theories and models related to technology adoption, such as the Diffusion of Innovation theory by Rogers (2003), or the Technology Acceptance Model by Venkatesh et al. (2003). However, what sets the PPM theory apart is its flexibility and its broad focus on switching behaviour, unlike other frameworks that only explore behavioural aspects of technology adoption (Nayak et al., 2022). Additionally, the theory has already been used to describe cybersecurity considerations during the adoption of new technologies during a study done by Lenz et al. (2023). Therefore, it is well suited to look at different factors that influenced the final decision made during the procurement of new medical devices in hospitals.

The PPM theory consists of three different components: push factors, pull factors, and mooring factors (Lenz et al., 2023; Nayak et al., 2022). Originally, push factors were defined as factors that motivate people to leave their place of origin. Conversely, pull factors attract people to a certain destination. Mooring factors facilitate or inhibit the migration to the new destination, either due to personal or social factors. In the context of technology switching behaviour, push factors push users away from their current technology, whilst pull factors attract them to new technologies. Mooring factors either facilitate or inhibit the user's transition to new technologies. The PPM theory applied to technology switching behaviour, is summarised in Table 15 below.

Table 15 - Push-Pull-Mooring definitions

Factors	*Description*
Push factor	Factors that push users away from the current technology they are using.
Pull factor	Factors that attract users to the adoption of new technology.
Mooring factor	Factors that either inhibit or facilitate a user's switching intentions to new technology

In this study, this theory can be used to explain the factors that cause hospitals to steer away from their current medical device, and why they choose for a certain other device. Thereby it can explain if and how cybersecurity plays a role when procuring new medical devices in hospitals.

6.1.2 Complex Decision-Making Framework

As Jalali & Kaiser (2018) conclude, hospitals can be viewed as complex systems with many different actors involved. To analyse the decision-making process in such complex environments, Nyhlén & Lidén (2014) developed the complex decision-making (CDM) framework. Initially developed for studying political decisions, Nyhlén & Lidén (2014) used a systems thinking approach to incorporate both micro and macro levels involved in the decision-making progress. This resulted in the distinction of two dimensions that influence the decision-making process. The first dimension includes structural conditions and actor-oriented explanations. Structural conditions cannot cause change in themselves; however, they are defined as potential influences on the behaviour of individuals, and thereby their decision-making as well. On the other hand, actor-oriented explanations focus on the actions of individual actors on the decision-making process. The second dimension differentiates between an exogenous or endogenous origin of the structure or actor. In the case of this study, this results in structures or actor coming from within the hospital or outside. This results in the framework depicted in Table 16 below.

Table 16 – Components of the Complex Decision-Making Framework (Nyhlén & Lidén, 2014)

	Structural conditions	*Actor-oriented explanations*
Exogenous	Exogenous structural conditions	Exogenous actors-oriented explanations
Endogenous	Endogenous structural conditions	Endogenous actors-oriented explanations

Exogenous structural conditions are macro variables and can defined as characteristics of the whole society. On the other hand, endogenous structures are traits such as cultures, norms, and values. Furthermore, it can encompass hard data, such as the organisation's internal economic conditions. Nyhlén & Lidén (2014) also exemplify this as how the organisational culture can impact the decision-making process. Exogenous actor-oriented explanations are actors outside of the decision-making process influencing the decision-making inside an organisation. As an example, Nyhlén & Lidén (2014) discuss how citizens might demand their politicians to implement a certain policy. Finally, endogenous actor-oriented explanations are the convictions and beliefs of the actors directly contributing to the decision-making process. This results in a more detailed framework, shown in Table 17 below.

Table 17 - Detailed Complex Decision-Making Framework

	Structural conditions	*Actor-oriented explanations*
Exogenous	Characteristics of the society	Outside actors influencing the decision-making process
Endogenous	Organisational culture Norms and values Internal economic conditions	Convictions and beliefs of internal actors associated with the decision-making process

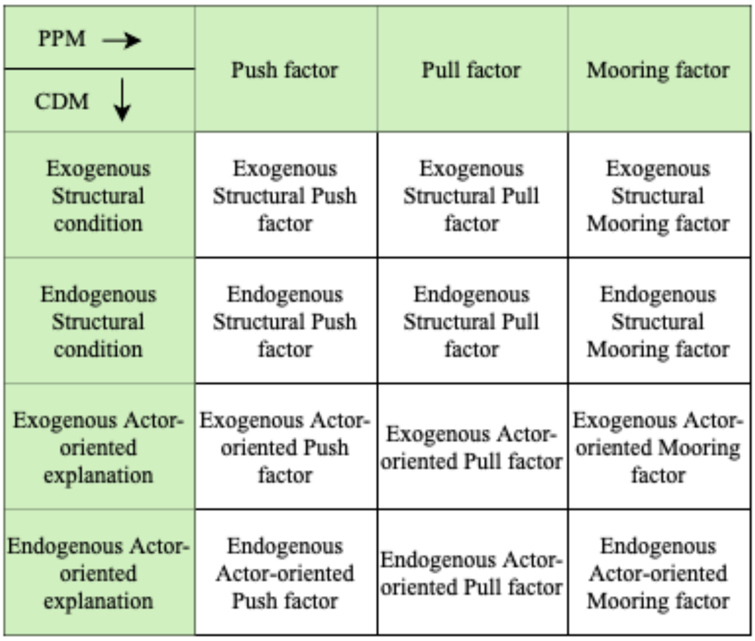
In this study, this framework can be used to analyse the complex interaction within procurement processes in Dutch hospitals and can provide a richer overview of the micro and macro interactions during procurement.

6.1.3 A combined approach

Although the PPM theory is very well suited to explain on a high-level how cybersecurity could play a role when switching to new medical devices, its focus lies more on individual behaviour. Therefore, it is not well suited to explain the complex intricacies of the complex procurement process in hospitals that involve many different stakeholders. On the other hand, the CDM framework provides a detailed explanation of how decisions are made, including micro and macro interactions within the procurement process. However, due to its origin in political science, it lacks the focus on technology, and more specifically, switching behaviour.

Therefore, a combined approach of the PPM theory and CDM framework is proposed, to provide a richer definition of the role of cybersecurity during the procurement of medical devices. In a way the CDM framework will explain how the intricacies of the decision-making process can lead to different PPM factors. Vice versa, the PPM factors are explained by the CDM framework in terms of how they can influence the decision-making process.

The combination of the PPM theory and CDM framework resulted in 12 different factors that can be used to explain the role of cybersecurity, or other considerations made during the procurement process. This was achieved by assigning a push, pull, and mooring factor to the structural conditions and actor-oriented explanations of the CDM framework. This is shown in Figure 13 below.



PPM → CDM ↓	Push factor	Pull factor	Mooring factor
Exogenous Structural condition	Exogenous Structural Push factor	Exogenous Structural Pull factor	Exogenous Structural Mooring factor
Endogenous Structural condition	Endogenous Structural Push factor	Endogenous Structural Pull factor	Endogenous Structural Mooring factor
Exogenous Actor-oriented explanation	Exogenous Actor-oriented Push factor	Exogenous Actor-oriented Pull factor	Exogenous Actor-oriented Mooring factor
Endogenous Actor-oriented explanation	Endogenous Actor-oriented Push factor	Endogenous Actor-oriented Pull factor	Endogenous Actor-oriented Mooring factor

Figure 13 - Combination of the CDM framework and PPM theory

These factors are detailed and defined in the context of hospitals in Table 18 below.

Table 18 - Combined theoretical approach definitions

No.	*Factor*	*Definition*
1	Exogenous Structural Push factor	A characteristic from society or the hospital sector that pushes a hospital away from the current device they are using.
2	Exogenous Structural Pull factor	A characteristic from society or the hospital sector that pulls a hospital toward the adoption of a new device.
3	Exogenous Structural Mooring factor	A characteristic from society or the hospital sector that inhibits or facilitates the hospital's switching intentions to a new device.
4	Endogenous Structural Push factor	Internal culture, norm, value or economic condition that pushes a hospital away from the current device they are using.
5	Endogenous Structural Pull Factor	Internal culture, norm, value or economic condition that pulls a hospital toward the adoption of a new device.
6	Endogenous Structural Mooring factor	Internal culture, norm, value or economic condition that inhibits or facilitates the hospital's switching intentions to a new device.
7	Exogenous Actor-oriented Push factor	An outside actor that influences the hospital away from the current device they are using.
8	Exogenous Actor-oriented Pull factor	An outside actor that influences the hospital to adopt a new device.
9	Exogenous Actor-oriented Mooring factor	An outside actor that inhibits or facilitates the hospital's switching intentions to a new device.
10	Endogenous Actor-oriented Push factor	Convictions and beliefs of internal actors that push a hospital away from the current device they are using.
11	Endogenous Actor-oriented Pull factor	Convictions and beliefs of internal actors that pull a hospital toward the adoption of a new device.
12	Endogenous Actor-oriented Mooring factor	Convictions and beliefs of internal actors that inhibit or facilitate the hospital's switching intentions to a new device.

6.2 Defining the factors for procurement

In section 4.3.2 different reasons for initiating a procurement process were discussed, whilst section 4.3.4 defined different requirements for medical devices during the procurement process. As cybersecurity can be both a consideration prior to the start of the procurement process and during the process, both are discussed in this chapter. To be able to identify the role cybersecurity plays in the procurement process, the combined approach as described in the previous section is applied. The result of this is discussed for the procurement initiation and the requirements below.

6.2.1 Procurement initiation

This section applies the theoretical lens to the identified reasons for procurement initiation.

Internal stakeholders

Internal stakeholders, such as the clinical physicist, MedTech department, IT Department or the 'owner' of a medical device can all start a new procurement process, when they think it is needed. This can either be based on their belief that a certain device is outdated, or because they belief that a new device can be of added benefit to the hospital. Therefore, it can be both an *endogenous actor-oriented push factor* and an *endogenous actor-oriented pull factor*.

Dissatisfaction with medical devices

Dissatisfaction with current medical devices in use in a hospital can be a reason to switch to a new device. As this is based on the beliefs of the internal stakeholders, this can be defined as an *endogenous actor-oriented push factor*.

End-of-life of medical device

All devices in use in a hospital have a certain lifespan. Each device is replaced at a regular interval, for example every 10 years. As this is related to the internal economic situation of the hospital, this can be defined as an *endogenous structural push factor*.

Guidelines

New guidelines set by, for example, the Dutch health authority or a medical specialists association can dictate the use of certain devices if a hospital wants to perform a certain procedure. This can therefore influence a hospital to adopt a certain new device. As these guidelines come from outside of the hospital and are sector wide, this can be defined as an *exogenous structural pull factor*.

Hospital rivalry

There is a certain rivalry between hospitals and doctors to give the best care possible. This can lead to doctors boasting about the new devices they just got, which in return can influence other doctors to also want new devices to keep up with the other hospitals and doctors. H1.P2 described is as follows: "*And as doctors amongst yourselves, (...) it was kind of a macho thing. 'What new device do you have? Oh, you don't have anything new? I'll pay for dessert then.*" As this results in outside actors influencing the start of a new procurement process, it can be defined as an *exogenous actor-oriented pull factor*.

New medical treatment

Sometimes, new treatments for a disease require a new device. This can be because it is a completely new device, or because the current devices lack a certain feature. As this is based on external developments in the healthcare sector, it can be defined as an *exogenous structural pull factor*.

New technology on the market

Medical devices are in continuous development, which leads to them improving over time with new functions and improved capabilities. This can persuade hospitals to adopt a new device when they think the improvements are of added value to the hospital. As this is based on developments in the healthcare sector, it can be defined as an *exogenous structural pull factor*.

6.2.2 Requirements

This section applies the theoretical lens to the identified requirements for new medical devices set by the hospitals during the procurement process.

Aftersales

The aftersales requirement focusses on the services the manufacturers offer after the device has been installed. This could be the availability of spare parts, but also the provision of instructions to users. This requirement mostly comes from the medical technology department and clinical physicists within the hospital, as they are the ones that have to do the repairs. Therefore, it can be deemed an *endogenous actor-oriented pull factor*, as from the interviews it can be concluded that this is an important requirement that can influence the decision for a certain device. For example, H2.P1 mentioned: "*(...) if we simply have bad experiences with suppliers from our department and we can substantiate that, then we would also like to include that in our technical advice. And in that respect we are simply a full-fledged discussion partner, so from the user's point of view, the user also benefits from the fact that no matter how beautiful a device is, it also benefits from the moment that you experience problems and malfunctions, it is picked up in a correct manner (...)".* However, it is not an endogenous actor-oriented push factor, as H1.P2 mentioned that even when the aftersales were unsatisfactory, the problems with the manufacturer were always resolved.

Cleanability

Cleanability refers to the way the devices can be cleaned. For example, whether they can withstand 70% alcohol when they are cleaned. This requirement is set by the infection prevention specialist at the hospital who evaluates how devices should be cleaned and if they adhere to the hospital's protocols. Therefore, it is an *endogenous structural mooring factor*, as this can inhibit the switching intentions when new devices do not comply.

Compatibility with other systems

Medical devices should be able to work with the other (IT) systems at the hospital, such as an electronic patient file. Therefore, hospitals will consider this when buying a new device. H1.P2 recalls a time when their devices were not compatible with their electronic patient file system: "*So well, we had those devices, but we didn't have the drivers for them because it wasn't ready yet and had to come all the way from America."* As this compatibility with systems is crucial for hospitals, it can be considered an *endogenous structural push factor* when devices are not compatible, so hospitals will find a way to ensure this compatibility.

Cybersecurity

As discussed in section 4.3.4, there are numerous cybersecurity requirements that hospitals set for new medical devices. These requirements come from two different sources. First, regulations dictate the minimum cybersecurity requirements that hospitals and medical devices should follow. Second, hospitals have their own cybersecurity policy and infrastructure that devices need to be compatible with. H2.P1 summarised it as: "*It must fit within H2's infrastructure and it must fit within the laws and regulations, so to speak*." However, when asked whether cybersecurity could be a reason to choose one device over another or be a reason to start a procurement process at all, all interviewees agreed that this was not the case. Consequently, hospitals see cybersecurity as a knock-off criterium. A device should comply with the requirements set, but it does not matter if it performs better on cybersecurity than another device. H2.P1 mentioned: "*Yes, it must meet [cybersecurity requirements]. That is the starting point. So, it must comply. But it doesn't really matter if something is extra safe or extra well protected."* Therefore, it can be defined both as an *endogenous structural mooring factor* and an *exogenous structural mooring factor*, as it inhibits switching intentions when new devices do not comply with policies set by either internal stakeholder, or by regulatory bodies.

Data security

All hospitals consider the security of the data they generate. For example, that the data should be encrypted, and if the data is processed by an external provider, that it does not leave the EU. As discussed in section 3.1.3, this has most likely to do with the requirements set by the GDPR. However, no interviewee mentioned it as a defining factor during the procurement process. Therefore, it is an *exogenous structural mooring factor*, as it is caused by external regulations and can inhibit the selection of a certain device when it does not comply with this requirement.

Price

Price is, of course, an important consideration during the procurement process. Devices can only be bought that fall within the budgetary restrictions of the hospital, and specifically the department. Not only the upfront cost of the device is considered, but also the total cost of ownership, which includes the costs for repairs and such. Therefore, it can be seen as an *endogenous structural mooring factor*. As the price of a new device can inhibit the switching intentions when they are too high.

Regulation compliance

All devices that operate within a hospital should be compliant with the relevant regulations, such as the MDR and CE mark. Therefore, hospitals will always check whether new devices they procure follow these regulations and have the relevant certifications. Consequently, it can be defined as an *exogenous structural push factor* when the current devices do not adhere anymore to more stringent current regulations.

Reliability

Medical devices in hospitals should work, and hospitals should be able to rely on them to continue to work. Therefore, it can be an *endogenous structural push factor* when the current devices become old and unreliable. However, it can also be an *exogenous actor-oriented mooring factor* during the procurement process of a new device. Hospitals may check with other hospitals what their experiences are with a certain device. As H1.P2 states: "*The technical department calls colleagues from another hospital, and asks: what is your experience with the device? Does it break often?"* Therefore, these experiences from other hospitals can either facilitate or inhibit the switching intentions, based on whether they are positive or negative.

Repairability

Repairability is closely related to the aftersales requirement, as it also includes the availability of spare parts. However, it is more focussed on the ability of the hospital to repair the device themselves, instead of relying on the manufacturer to service the device. These requirements are often set by the medical technology department that evaluates the device. Although during the interviews there was no mention of this being a specific push or pull reason for their current device, it is considered during the evaluation process of a new device. Therefore, it is an *endogenous actor-oriented mooring factor*.

Safety

Safety is focussed on the safe operations of medical devices. This could be related to their electrical circuits, but also radiation. These requirements are set by outside actors in the form of certain certifications a device should have, but also by the medical technology department of a hospital. The latter checks if the devices comply with those certifications and check the device themselves. Although it could be possible that devices are bought because the old device does not comply with new regulations, this did not come forward during the interviews. Therefore, it is both an *endogenous actor-oriented mooring factor* and an *exogenous structural mooring factor*, as it is not a reason to buy a certain device but can inhibit the switching intentions when new devices do not have the right certifications.

Supplier satisfaction

When hospitals buy new medical devices, their previous experience with a certain supplier can influence the procurement process. This could lead to a certain supplier not being considered during the process, as their services were unsatisfactory. Similarly to the aftersales requirement, this is based on the experiences of the internal stakeholders of the hospital and can steer the hospital to a certain device, it can be defined as an *endogenous actor-oriented pull factor*.

6.3 Answering sub question 4

This section will provide an answer to SQ4: *How are cybersecurity aspects considered compared to other considerations during the procurement of new medical devices?*

The reasons for a procurement initiation and the requirements for new medical devices are summarised in Table 19 below, in the context of the theoretical lens proposed in this chapter.

Table 19 - Procurement factors

Procurement process	*Factor*
Procurement initiation	
Internal stakeholders	Endogenous actor-oriented push factor
	Endogenous actor-oriented pull factor
Dissatisfaction with medical devices	Endogenous actor-oriented push factor
End-of-life of medical device	Endogenous structural push factor
Guidelines	Exogenous structural pull factor
Hospital rivalry	Exogenous actor-oriented pull factor

New medical treatment	Exogenous structural pull factor
New technology on the market	Exogenous structural pull factor
Requirements	
Aftersales	Endogenous actor-oriented pull factor
Cleanability	Endogenous structural mooring factor
Compatibility with other systems	Endogenous structural push factor
Cybersecurity	Endogenous structural mooring factor
	Exogenous structural mooring factor
Data security	Exogenous structural mooring factor
Price	Endogenous structural mooring factor
Regulation compliance	Exogenous structural push factor
Reliability	Endogenous structural push factor
	Exogenous actor-oriented mooring factor
Repairability	Endogenous actor-oriented mooring factor
Safety	Endogenous actor-oriented mooring factor
	Exogenous structural mooring factor
Supplier satisfaction	Endogenous actor-oriented pull factor

In conclusion, based on the interview quotes presented throughout this thesis, the role of cybersecurity in the procurement process of new medical devices, although present, is not a primary driving factor. Through the combined application of the PPM theory and CDM framework, it has been illustrated that the procurement process is of a multifaceted nature. Cybersecurity requirements are seen primarily as mooring factors, both endogenous and exogenous, which means they act as baseline criteria that must be met but do not significantly influence the selection among satisfactory options, nor is it a reason to initiate a procurement process.

Internal stakeholders initiate procurement processes based on a variety of factors including dissatisfaction with current devices, end-of-life considerations, and the influence of new guidelines, treatments, and technologies. Cybersecurity considerations originate from both regulatory requirements and internal policies but are typically viewed as necessary compliance checks rather than competitive advantages, as no interviewee determined it as a crucial factor during the decision process.

In summary, while cybersecurity is crucial for ensuring the safe and secure operation of medical devices, it functions more as a foundational requirement rather than a differentiating factor in the decision-making process. Hospitals prioritise other requirements such as compatibility, reliability, and compliance with broader regulatory and institutional standards, considering cybersecurity as an essential, yet secondary criterion within the procurement process.

7 Recommendations for hospitals

This chapter will provide recommendations to improve the role of cybersecurity based on the findings of this thesis. By doing so, it will answer SQ5: *What recommendations can be derived to improve the role of cybersecurity during the procurement process of new medical devices in Dutch hospitals, if at all?*

7.1 Cybersecurity awareness

From the findings of this thesis one primary recommendation can be derived: creating cybersecurity awareness amongst all participating stakeholders within the hospital. The reason for this is the current discrepancy between stakeholders on the importance of cybersecurity within hospitals and during the final decision making. From this study it can be concluded that the final decision is made in consultation with all the different stakeholders involved during the process. Here, everyone can voice their preference based on their expertise. In the case that no final consensus can be made, the wishes of the end-user can be decisive. However, often these wishes are focussed on work efficiency instead of on cybersecurity measures that could potentially hamper their workflow. Similarly, other stakeholders primarily focus on their own expertise. Therefore, if all stakeholders involved in the decision-making process are made aware of the importance of cybersecurity, they might value it more and incorporate it in their preferences for a device. This is in contrast with how it is now, where only the IT department is concerned with incorporating cybersecurity considerations in their preference.

This recommendation is also mentioned by one of the cybersecurity specialist, E1.P1, interviewed for this thesis. This participant mentioned: *"[The average healthcare professionals] just want to help people. That's what it comes down to and everything you do as a security professional often makes that more difficult, so it's very difficult to find a balance in like, well, how do we make sure we're still safe, without medical staff feeling inhibited in being able to do their job and so there's a technical piece of challenge in that. (...) And so also a bit of education, right? How do you get that medical staff to understand why we do that?"*

7.2 Include higher management

The second recommendation focusses on a bigger role for higher management during the procurement process. During the interviews conducted for this thesis, higher management was barely mentioned. However, higher management is in the unique position to oversee the procurement process and ensure that the interests of the hospital are protected. If higher management is made aware of the importance of cybersecurity, they could voice this importance during the procurement process to the other stakeholders involved. This could also persuade the other stakeholders to understand the importance of cybersecurity, which in return improves the role cybersecurity plays during the procurement process.

This heightened responsibility for higher management to understand and advance cybersecurity is also part of the new NIS2 directive introduced in the EU. Therefore, this recommendation is mostly in line with that directive. Yet, as it is a directive it is unsure how this will be transposed into Dutch law. Lawmakers should therefore take this recommendation into consideration and make sure that this part of the NIS2 directive is closely matched in the to be introduced Dutch law.

7.3 Combine departments

The third recommendation focusses on combining the MedTech department and the IT department. In Hospital 2 these two departments were merged, as they noticed that due to the increasing digitalization of devices they became more codependent of each other. This also resulted in one preference voiced during the final decision-making process based on the technical aspects of the devices. The introduction of such a singular preference based on the technical capabilities of a device could strengthen their voice during the decision-making process. In return, this can result in the improvement of the role of cybersecurity during the procurement process if this 'technical' voice is appreciated by the other stakeholders involved during the procurement process.

7.4 Cybersecurity evaluation

The final recommendation is focused on evaluation. During the interviews it became apparent that sometimes the procurement process is evaluated afterwards. This evaluation is then used in the future to enhance the procurement process. Similarly, the cybersecurity of devices could also be evaluated. This could either be done by the hospital itself or a third-party specialist. This evaluation could even cover the whole hospital network and pinpoint the most vulnerable devices in the network. This knowledge could then be used during the procurement process to base the cybersecurity requirements on.

As was mentioned in previous chapters, cybersecurity is often regarded as a baseline requirement, devices should meet certain standard requirements, but do not need to perform better. The knowledge gained from the cybersecurity evaluations could lead to new minimum requirements being set, which in return could improve the cybersecurity of the devices being procured.

To conclude, when there is a consensus within the organisation on the importance of cybersecurity, cybersecurity requirements might be prioritised more during the procurement process. This would result in cybersecurity not just being 'added' after the device has been procured but considered from the start by hospitals and therefore better represented in the program of requirements. If more hospitals include this in their program of requirements, it will also move manufacturers to think even more about the cybersecurity of their devices. This will result in even better cybersecurity within hospitals.

8 Discussion

This chapter will provide a short summary of the main findings of this thesis and will elaborate on how it aids in fulfilling the knowledge gaps found in chapter 1.2.3. Afterwards, it will go over the limitations of this thesis, followed by future research recommendations based on this study and a reflection on the process of this research.

This study delved into the procurement practices of medical devices in Dutch hospitals, with a keen focus on how cybersecurity considerations are integrated into these processes. It revealed that the procurement process is multifaceted, involving various stakeholders such as doctors, IT staff, procurement departments, amongst others. The process typically starts with market exploration and the creation of a program of requirements, followed by the issuance of requests for proposals, rigorous evaluation of these proposals, and detailed contract negotiations. Despite the structured nature of this process, the integration of cybersecurity considerations is found to be a baseline requirement. Devices should meet the requirements set, but if a device excels on cybersecurity, this isn't viewed as an added benefit.

External influences can play a role in shaping procurement decisions. Manufacturers actively engage with doctors and hospital staff, often providing trial installations to demonstrate the capabilities of their devices. Medical conferences and peer opinions from doctors in other hospitals can also influence procurement choices.

This thesis identified two knowledge gaps in the beginning: the limited understanding of medical device procurement in Dutch hospitals and the lack of knowledge on how cybersecurity is integrated into these processes.

Regarding the first knowledge gap, this study a comprehensive analysis of the current procurement practices for medical devices in Dutch hospitals. By detailing the stages of procurement, from market exploration to contract negotiations and evaluation, the research offers a clear depiction of the complexities and stakeholder dynamics involved. This in-depth understanding is crucial for both practitioners and researchers who aim to improve procurement efficiency and outcomes in the healthcare sector.

However, one of the most critical contributions of this thesis is its focus on the integration of cybersecurity considerations into the procurement process. The research highlights that, although present, cybersecurity considerations remain marginal during the procurement process. Cybersecurity is often set as a baseline requirement and is often not considered beyond that. Instead, cybersecurity is often 'added' to the device afterwards, for example by placing it in a segmented network. This, despite the growing digitalisation of medical devices and the associated risks. In part, this might be due to the lack of specific regulations on this topic. Therefore, the study underscores the need for hospitals to adopt more structured and standardized approaches to cybersecurity in procurement.

Looking back at the considerations found during the initial literature review done for this thesis, summarised in Table 2 - Procurement considerations found in the literature, this thesis has found several similar considerations. More specifically, the considerations economic, physical/technical aspects, interoperability within hospital, clinical data, end user preference, provider reputation and relation, and experiences of other doctors. These were also mentioned during the interviews of this thesis, albeit that clinical data is incorporated into the regulation compliance requirement. The other seven considerations found during the literature review, were not directly mentioned by the participants. Yet, this thesis adds three more considerations to the literature: aftersales, cybersecurity, and data security.

To conclude, this thesis contributed scientifically to the domain of process analyses, specifically regarding procurement processes in the context of Dutch hospitals. Consequently, researchers within this domain may utilise the findings from this thesis to improve their comprehension of the procurement process in Dutch hospitals. Furthermore, they could build upon this thesis based on the recommendations for future research discussed in section 8.2 or based upon a researcher's own merits or interests.

8.1 Limitations

This thesis, whilst still relevant, has several limitations. Most of these limitations come from the time constraints of this thesis and the research methods used. The limitations are elaborated upon below.

8.1.1 Master thesis limitations

The primary limitation of this thesis lies in the restricted timeframe within which it was developed. This restricted timeframe may have impacted the depth of research, analysis, and the variety of perspectives considered. Additionally, although this research effort was well guided by experienced researchers, the inexperience of this author as a Master student is not to be overlooked. This might have impacted the research results to some degree.

8.1.2 Desk research limitations

The desk research conducted for this thesis is constrained by the availability and reliability of the sources accessed. Depending on the accessibility of academic databases, sector data, and institutional libraries, certain relevant literature or data may not have been accessible, potentially limiting the complete view on the research topic. Additionally, the topics covered in academic literature, and the depth of analysis provided by existing scholarly works may vary, potentially resulting in gaps or limitations in understanding certain aspects of the research topic. The selection of sources may also be influenced by inherent biases, such as the researcher's preferences, familiarity with certain authors or journals, or the accessibility of specific types of literature. Consequently, there is a risk that the literature review may not fully represent the full array of perspectives or alternative viewpoints relevant to this thesis. This is, for example, evident in the search query used for the literature review, where a deliberate choice was made to phrase the query using ‘procurement’ instead of alternatives such as ‘acquiring’. Finally, researcher bias is also evident not only in the literature accessed, but also in the way this research is interpreted by this researcher.

8.1.3 Interview limitations

The use of semi-structured interviews has allowed this research to gather first-hand experience of stakeholders that are directly or indirectly involved in the procurement process. However, the use of these interviews does introduce some limitations. First, the limited number of interviews conducted, with six hospital interviews, and one external stakeholder interview may negatively affect the reliability and generalisability of the results. This especially holds true for the external stakeholders, where only one organisation agreed to an interview. Additionally, manufacturers were not considered in the sample, whilst they do play an important role in the procurement process. Including their view might have put the conclusion in a new light. Therefore, this is interesting for future research, see section 8.2.2. Finally, the sample included stakeholders with different roles across the different hospitals. This makes the direct comparison between hospitals less robust, as the stakeholders might look differently towards the procurement process.

The use of semi-structured interviews also introduces bias into this research. First, bias can be introduced by the small sample of participants that contributed to this study that all have their own opinions on the procurement process. Including more participants would have limited the influence of one stakeholder on the outcomes of this study. Second, bias is introduced by the researcher. The interview transcripts were coded by one single researcher, without a second opinion on the codes. Despite efforts to maintain objectivity, this could still introduce bias in the way the transcripts are interpreted by the researcher. Next to this, the interview protocol was created by the same interviewer, which might lead to the interviewer steering the conversation toward desired results. Although the interview protocol received feedback from the thesis committee, the risk of bias still prevails.

8.2 Future research recommendations

This thesis has provided insight into possible future research endeavours. These recommendations are detailed below, including potential future research questions.

8.2.1 Academic hospitals

From the institutional environment analysis, but also during the interviews, it became apparent that academic hospitals are tender compliant, whereas non-academic hospitals are not. This leaves the possibility to research not only how this affects the procurement process in academic hospitals, but also how the role of cybersecurity might be affected by this. Additionally, as tenders must be public, the opportunity to perform a tender analysis arises. In this analysis, the requirements for cybersecurity can be studied and compared to the other requirements set out by academic hospitals, to determine the role of cybersecurity within the process.

Potential research questions:

1. How does tender compliance impact the procurement process in Dutch academic hospitals?
2. How does the procurement process differ between academic and non-academic hospitals in the Netherlands?
3. To what extent do cybersecurity requirements outlined in public tenders for medical devices align with the broader institutional priorities and objectives set out by academic hospitals

8.2.2 Medical device manufacturers

Based on the results of this thesis it can be concluded that manufacturers can play a big role in persuading hospitals to choose for a certain medical device, albeit only because of the satisfaction hospitals have with a certain manufacturer. Therefore, it could be interesting to include the view of manufacturers on this topic. This gives a range of ways to look at the problem. For example, how manufacturers look at cybersecurity for their medical devices; Do they find it important? Are the regulations too stringent, or not stringent enough? But it also gives way to study how manufacturers look at the importance of cybersecurity during the procurement process and if it is part of their sales pitch. Additionally, it could be studied how hospitals and manufacturers perceive where the responsibility lies for the cybersecure operations of a device.

Potential research questions:

1. How do medical device manufacturers perceive the importance of cybersecurity in the design and development of their products, and what factors influence their prioritisation of cybersecurity features?
2. To what extent do medical device manufacturers believe that current regulations adequately address cybersecurity concerns in the healthcare sector?
3. What strategies do medical device manufacturers employ to integrate cybersecurity considerations into their products' procurement process
4. How do medical device manufacturers perceive the role of collaboration with healthcare institutions in enhancing cybersecurity practices and responsibility?

8.2.3 Stakeholder dynamics

The focus of this study was on the variety of stakeholders interviewed across multiple hospitals. From these interviews it became clear that the different stakeholders all have a different view on the importance of cybersecurity, and cybersecurity in general. This leaves the opportunity to focus on one hospital as a single case study and to investigate the perspectives of different stakeholders from within the hospital on cybersecurity. This can be in regard of the procurement process, but also in general. For example, multiple participants mentioned that some stakeholders do not want to be inhibited by cybersecurity measures, whilst others think that cybersecurity should be a high priority. Therefore, a study could focus on the views of different stakeholders on cybersecurity and delineate any potential pain points for wide cybersecurity acceptance.

Potential research questions:

1. How do the attitudes and priorities of different stakeholders within a hospital towards cybersecurity vary, and what factors contribute to these variations?
2. How do stakeholders within a hospital perceive the trade-offs between cybersecurity measures and operational efficiency, and what strategies can be implemented to reconcile these potentially conflicting priorities?

8.2.4 Comparison with other EU countries

The geographic scope for this study was centred on the Netherlands. However, a lot of regulations that manufacturers or hospitals need to follow are EU-based. Therefore, it could be interesting to look at how these regulations affect hospitals in other EU countries. Additionally, as manufacturers operate on an international scale, cybersecurity considerations during the procurement process in one country could affect other countries when this introduces new security measures for the device being sold. Consequently, it could be studied how hospitals in other EU countries shape their procurement process and how cybersecurity is considered during this process.

Potential research questions:

1. How do EU healthcare regulations impact the procurement process and cybersecurity considerations in hospitals in different EU countries, and what are the common challenges and disparities encountered by healthcare institutions across various national contexts?
2. How does hospital cybersecurity regulations in one EU country affect other EU countries?

8.2.5 Introduction of NIS2

As discussed in Chapter 3, the introduction of NIS2 could influence the procurement process in several ways. For example, so called management bodies could become more involved during the procurement process. In addition, it would oblige hospitals to assess the cybersecurity of their suppliers and service providers. Therefore, once the NIS2 has been transposed into Dutch law, it could be interesting to research the effect the directive has on the procurement process and hospitals in general.

Potential research questions:

1. What changes have been observed in the procurement processes of Dutch hospitals following the transposition of NIS2 into national law?
2. How are Dutch hospitals assessing the cybersecurity measures of their suppliers and service providers in compliance with NIS2?
3. How does the introduction of NIS2 influence the involvement of management bodies in the procurement process within Dutch hospitals?

8.3 Personal reflection

The process that led to finalising this journey can be described as thrilling, enlightening, and impactful on me as a researcher. It provided not only a deeper understanding of the topic, but also an appreciation of the research process.

One of my main lessons was to keep being flexible and to adapt to changes, whilst remaining a clear structure and schedule. Due to some delays in the Human Research Ethics approval process, my ability to contact potential participants was also delayed. This meant that I could start contacting participants in a relatively late stage of my thesis, whilst the healthcare sector is notoriously busy and overworked. However, this has taught me to remain flexible to be able to adjust to the schedule of the participants. This also meant that I had to adjust my own planning for my thesis I made beforehand. Yet, by making these changes to the schedule, it allowed me to keep on track for the thesis deadline. Therefore, the importance of a clear schedule and structure for yourself became once again apparent to me.

A second lesson I learned was the importance of scoping my research down to a level that will deliver clear results. At the beginning of this thesis, my goal was too ambitious and too broad, which would have led to unclear results. In part, my broad interest might be to blame, which occasionally led me to be distracted with the less important stuff. So, during the research process I learned to keep focus on what is important now, and to delve into the other topics when needed.

Third, I learned to trust the research process, with all its associated ups and downs. At times, I could be stuck on a certain topic, or was unsure what to do next. However, especially these moments were insightful, as it taught me to break the problem down in smaller parts. Solving each smaller part, will eventually lead to solving the sum of it all. These tiny wins, make the problem seem smaller and more manageable.

When I reflect on the research methods chosen, I can conclude that the framework analysis potentially wasn’t necessary, as the procurement processes per hospitals only differ in the details. When I started my research efforts, I assumed that there would be large differences between hospitals on how they look at cybersecurity during the procurement process. However, it turned out that these processes were mostly the same across the different hospitals. Therefore, just coding would have been enough. Yet, I don’t regret using the framework analysis, as it does provide a comprehensive overview of the differences that still exist between hospitals. Additionally, the framework analysis method was new to me, which required me to dive into it deeper and learn new things, which I always enjoy doing.

Finally, when I reflect on the theoretical lens used to compare the different requirements and reasons to initiate a new procurement process, I can conclude that it was better suited for describing reasons for a new procurement process than requirements. Although it was applicable to both, a lot of the requirements set during the procurement process are knock-out criteria rather than ways to compare devices with each other. This resulted in a lot of requirements being mooring factors, whilst nuances still exist. Yet, I think that the combination of the PPM theory and the CDM framework worked well, and I enjoyed reading into the vast diversity of different relevant theories before settling on this combination as the best one.

To conclude, the research process was an enlightening and dynamic journey that taught me new research methods, the need for flexibility, the importance of a clear structure and schedule, and the ability to tackle even the toughest of problems. These lessons will guide me in my future professional and academic endeavours.

9 Conclusion

This chapter will conclude this thesis. First, the main research question will be answered. Sections 9.2 and 9.3 will focus on the societal and scientific contribution of this thesis. Finally, the link to the CoSEM master programme will be emphasised in section 9.4.

9.1 Answering the main research question

This thesis set out to explore the current procurement practices for medical devices in Dutch hospitals, with a particular focus on how cybersecurity considerations are incorporated into these processes. This research was crucial given the increasing digitalisation of healthcare and the consequent rise in cyber threats that could pose significant risks to patient safety and data integrity. Despite the critical importance of cybersecurity, there was a notable gap in the literature regarding its integration into the procurement of medical devices within the Dutch healthcare context. This study aimed to fill this gap by providing a detailed examination of existing practices and offering insights into areas for improvement.

The research followed a structured approach, divided into five key phases. Initially, a comprehensive literature review was conducted to define the research problem and identify the knowledge gaps. This was followed by desk research to gain a detailed overview of existing policies, regulations, and scientific research related to procurement and cybersecurity in hospitals. Semi-structured interviews with stakeholders involved in the procurement process provided in-depth insights into current practices. These interviews were then analysed using a thematic framework to identify key themes and compare the different hospitals.

The study found that the procurement process in Dutch hospitals is complex and involves a wide variety of stakeholders within the hospital. External influences, such as manufacturers and peer opinions from doctors in other hospitals, also play a significant role. Despite the growing awareness of cybersecurity threats, its integration into procurement practices remains marginal. Hospitals typically prioritize functional and financial requirements over cybersecurity, treating it as a baseline requirement.

The main research question of this thesis was:

To what extent are cybersecurity considerations integrated into the procurement process of medical devices in Dutch hospitals?

To answer the main research question, the procurement practices for medical devices in Dutch hospitals involve a structured process influenced by both internal and external stakeholders. The process Dutch non-academic hospitals follow to procure new devices shows a striking resemblance across different hospitals. These practices prioritise factors such as device performance, cost, and compatibility, with cybersecurity being considered as a baseline requirement. Although cybersecurity is recognised as crucial for ensuring the safety and integrity of medical devices, it does not primarily drive procurement decisions. The influence of regulatory bodies and the need for compliance ensure that cybersecurity is addressed, albeit often as a complacency consideration. To enhance the integration of cybersecurity in procurement decisions, it is recommended that hospitals increase cybersecurity awareness among stakeholders and prioritise cybersecurity from the beginning of the procurement process. This approach can lead to a more balanced consideration of cybersecurity alongside other critical factors, ultimately improving the overall security posture of healthcare institutions.

In conclusion, this research provides a comprehensive overview of the current procurement practices for medical devices in Dutch hospitals and the extent to which cybersecurity considerations are incorporated. By addressing the identified gaps and offering practical recommendations, the study aims to enhance the security and resilience of healthcare systems in the face of evolving cyber threats. In addition, this thesis has contributed to society and science, which will be elaborated upon in the following sections.

9.2 Societal contribution

This thesis presents several societal contributions. By exploring and addressing the current procurement practices for medical devices in Dutch hospitals and the integration of cybersecurity considerations, this study contributes to various societal dimensions.

One of the primary societal benefits of this research is the enhancement of patient safety and data. Medical devices play a crucial role in diagnosing, treating, and monitoring patients. However, the increasing connectivity of these devices introduces cybersecurity risks that can directly impact patient safety and their data. By highlighting the importance of incorporating cybersecurity considerations into the procurement process, this thesis underscores the need for robust security measures to protect patients from potential harm caused by cyberattacks on medical devices. Improved procurement practices that prioritise cybersecurity can prevent future cyber-related incidents.

Second, the findings and recommendations of this thesis have the potential to inform policy and regulatory frameworks related to medical device procurement and cybersecurity. Policymakers and regulatory bodies can use the insights from this research to develop or refine regulations that mandate stronger cybersecurity measures for medical devices. This, in turn, can lead to a higher standard of security across the healthcare industry, benefiting society by reducing the risk of cyber threats and enhancing the overall security of hospitals.

Finally, the Dutch healthcare system is crucial, and its resilience to cyber threats is essential for maintaining public health and safety. This thesis contributes to building a more resilient healthcare system by promoting cybersecurity considerations in the procurement of medical devices. By ensuring that medical devices are secure from cyber threats, hospitals can maintain continuous and reliable healthcare services, even in the face of cyber incidents.

9.3 Scientific contribution

This thesis contributes scientifically in multiple ways. First, it addresses the knowledge gap found in section 1.2.3, by analysing the procurement practices in Dutch hospitals and mapping how cybersecurity is considered during this process. Additionally, this thesis provides several other contributions:

First, the interdisciplinary approach of this thesis, integrating technical, regulatory, and human factors, allows for a more holistic understanding of the challenges and opportunities on this topic. By bridging these different factors, this thesis highlights the connection between technical, managerial, and regulatory aspects. This more nuanced view can inform future academic discourse on the role of cybersecurity and inspire others to adopt a similar interdisciplinary approach.

Second, this thesis provides a novel conceptual framework to explain the role of cybersecurity during the procurement process. By combining the Push-Pull-Mooring theory with the Complex Decision-Making framework, a new way to analyse the procurement process of medical devices is presented. It highlights the complex nature of the decision-making process and explains how switching intentions can influence this process.

Third, a light is shed on the roles and influences of different stakeholders in the procurement process, including internal stakeholders (e.g., doctors, IT staff, hospital management) and external stakeholders (e.g., regulatory bodies, cybersecurity experts, manufacturers). By analysing how these stakeholders interact and influence procurement decisions, the thesis provides valuable insights into the dynamics of decision-making processes in Dutch hospitals.

Finally, by utilising a comparative case study approach of Dutch hospitals, this thesis provides detailed evidence on the current state of medical device procurement practices. The empirical findings reveal how hospitals prioritize various factors, including cybersecurity, and the extent to which external regulations and internal policies shape these practices.

9.4 Link to the CoSEM programme

This thesis studies the complexities of the decision-making that occurs during the procurement process of medical devices. During this analysis, the CoSEM perspective was used, which not only looked at the technical aspect, but also included regulatory, economic, and human factors in line with the complex nature of the decision-making process. This interdisciplinary approach resulted in the utilisation of insights from various fields, such as academia, law, and human factors. By doing so, this thesis provides a holistic analysis of the problem at hand in line with the emphasis of the CoSEM programme on a multi-faceted approach to analysing and solving technical challenges. Finally, this thesis underpins the socio-technical nature of the decision-making in the procurement process of new medical devices in hospitals where various factors and stakeholders need to be considered to come to the final conclusion.

References

Aanbestedingswet 2012 (2022). https://wetten.overheid.nl/BWBR0032203/2022-03-02

Ackermann, F., & Eden, C. (2011). Strategic Management of Stakeholders: Theory and Practice. *Long Range Planning*, *44*(3), 179–196. https://doi.org/10.1016/J.LRP.2010.08.001

Ahmed, M., & Barkat Ullah, A. S. S. M. (2018). False data injection attacks in healthcare. *Communications in Computer and Information Science*, *845*, 192–202. https://doi.org/10.1007/978-981-13-0292-3_12/FIGURES/1

Annas, G. J. (2003). HIPAA Regulations: A New Era of Medical-Record Privacy? . *The New England Journal of Medicine*, *348*(15). https://scholarship.law.bu.edu/faculty_scholarship

Aronson, J. K., Heneghan, C., & Ferner, R. E. (2020). Medical Devices: Definition, Classification, and Regulatory Implications. *Drug Safety*, *43*(2), 83–93. https://doi.org/10.1007/S40264-019-00878-3/TABLES/4

Baumer, D., Brande Earp, J., & Cobb Payton, F. (2000). Privacy of medical records: IT Implications of HIPAA. *ACM SIGCAS Computers and Society*, *157*(4), 258. https://doi.org/10.1145/572260.572261

Bhosale, K. S., Nenova, M., & Iliev, G. (2021). A study of cyber attacks: In the healthcare sector. *2021 6th Junior Conference on Lighting, Lighting 2021 - Proceedings*. https://doi.org/10.1109/LIGHTING49406.2021.9598947

Biasin, E., & Kamenjašević, E. (2022). Cybersecurity of medical devices: new challenges arising from the AI Act and NIS 2 Directive proposals. *International Cybersecurity Law Review 2022 3:1*, *3*(1), 163–180. https://doi.org/10.1365/S43439-022-00054-X

Billaux, M., Borget, I., Prognon, P., Pineau, J., & Martelli, N. (2015). Innovative medical devices and hospital decision making: a study comparing the views of hospital pharmacists and physicians. *Australian Health Review*, *40*(3), 257–261. https://doi.org/10.1071/AH15039

Blüher, M., Saunders, S. J., Mittard, V., Torrejon Torres, R., Davis, J. A., & Saunders, R. (2019). Critical Review of European Health-Economic Guidelines for the Health Technology Assessment of Medical Devices. *Frontiers in Medicine*, *6*, 499394. https://doi.org/10.3389/FMED.2019.00278/BIBTEX

Bosmans, H., Zanca, F., & Gelaude, F. (2021). Procurement, commissioning and QA of AI based solutions: An MPE's perspective on introducing AI in clinical practice. *Physica Medica*, *83*, 257–263. https://doi.org/10.1016/J.EJMP.2021.04.006

Boulding, H., & Hinrichs-Krapels, S. (2021). Factors influencing procurement behaviour and decision-making: an exploratory qualitative study in a UK healthcare provider. *BMC Health Services Research*, *21*(1), 1–11. https://doi.org/10.1186/S12913-021-07065-0/PEER-REVIEW

Brito Fernandes, Ó., Bos, V., Klazinga, N., & Kringos, D. (2022). Citizen engagement in healthcare procurement decision-making by healthcare insurers: recent experiences in the Netherlands. *Health Research Policy and Systems*, *20*(1), 1–10. https://doi.org/10.1186/S12961-022-00939-7/TABLES/3

Brookson, C., Cadzow, S., Eckmaier, R., Eschweiler, J., Gerber, B., Guarino, A., Rannenberg, K., Shamah, J., & Górniak, S. (2016). *Definition of Cybersecurity: Gaps and overlaps in standardisation*. https://doi.org/10.2824/4069

Bruggeman, E., Chao-Duivis, M. A. B., & Koning, A. Z. R. (2010). *A practical guide to Dutch building contracts* (4th edition). Instituut voor Bouwrecht (IBR).

Bryman, A. (2016). *Social Research Methods* (Fifth). Oxford University Press.

Bryson, J. M. (2007). *Public Management Review What to do when Stakeholders matter Stakeholder Identification and Analysis Techniques*. https://doi.org/10.1080/14719030410001675722

Callea, G., Armeni, P., Marsilio, M., Jommi, C., & Tarricone, R. (2017). The impact of HTA and procurement practices on the selection and prices of medical devices. *Social Science & Medicine*, *174*, 89–95. https://doi.org/10.1016/J.SOCSCIMED.2016.11.038

Callea, G., Federici, C., Ciani, O., Amatucci, F., Borsoi, L., Tarricone, R., & Marletta, M. (2020). Integrating HTA Principles into Procurement of Medical Devices: The Italian National HTA Programme for Medical Devices. *IFMBE Proceedings*, *76*, 1777–1782. https://doi.org/10.1007/978-3-030-31635-8_215/TABLES/2

Carrera, P. M., Katik, S., & Schotanus, F. (2015). Cooperative purchasing of pacemakers by Dutch hospitals: What are the determinants, cost-savings and perceived non-monetary benefits? *Proceedings of the 24th IPSERA Conference*.

Chartered Institute of Procurement & Supply. (n.d.). *What Is Procurement?* Retrieved March 4, 2024, from https://www.cips.org/intelligence-hub/procurement/what-is-procurement

Claroty, & Team82. (2024). *State of CPS Security Report: Healthcare 2023*. https://claroty.com/resources/reports/state-of-cps-security-report-healthcare-2023

Council of Europe, European Court of Human Rights, European Data Protection Supervisor, & European Union Agency for Fundamental Rights. (2018). *Handbook on European data protection law* (2018 edition). Publications Office of the European Union. https://data.europa.eu/doi/10.2811/58814

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, *113*, 48–52. https://doi.org/10.1016/J.MATURITAS.2018.04.008

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21. https://doi.org/10.22215/TIMREVIEW/835

Crowe, S., Cresswell, K., Robertson, A., Huby, G., Avery, A., & Sheikh, A. (2011). The case study approach. *BMC Medical Research Methodology*, *11*(1), 100. https://doi.org/10.1186/1471-2288-11-100

Dark Reading. (n.d.). *About Us | Dark Reading: Connecting The Cybersecurity Community*. Retrieved May 2, 2024, from https://www.darkreading.com/about-us

de Bruijn, H., & Janssen, M. (2017). Building Cybersecurity Awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), 1–7. https://doi.org/10.1016/J.GIQ.2017.02.007

Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on Public Procurement and Repealing Directive 2004/18/EC (2014). http://data.europa.eu/eli/dir/2014/24/oj

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive) (2022). http://data.europa.eu/eli/dir/2022/2555/oj

European Union Agency for Cybersecurity, Kyranoudi, P., Liveri, D., Drougkas, A., & Zisi, A. (2020). *Procurement guidelines for cybersecurity in hospitals: Good practices for the security of healthcare services*. https://doi.org/10.2824/943961

FDA. (2024, March 12). *Cybersecurity in Medical Devices Frequently Asked Questions (FAQs)* . https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity-medical-devices-frequently-asked-questions-faqs

FDA, U.S. Department of Health and Human Services, Center for Devices and Radiological Health, & Center for Biologics Evaluation and Research. (2023). *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions*. https://www.fda.gov/media/119933/download

FDA, U.S. Department of Health and Human Services, Center for Devices and Radiological Health, Office of the Center Director, & Center for Biologics Evaluation and Research. (2016). *Postmarket Management of Cybersecurity in Medical Devices*. https://www.fda.gov/media/95862/download

Fedorowicz, J., & Ray, A. W. (2004). Impact of HIPAA on the integrity of healthcare information. *Int. J. Healthcare Technology and Management*, *6*(2), 142–157.

Filiniuk, O., Babenko, M., Kosyachenko, K., & Sucu, R. (2023). Current approaches of health technologies introduction in Ukrainian hospitals. *ScienceRise: Pharmaceutical Science*, *2023*(5(45)), 16–23. https://doi.org/10.15587/2519-4852.2023.289683

Food, Drug, and Cosmetics Act (2018). https://www.fda.gov/regulatory-information/laws-enforced-fda/federal-food-drug-and-cosmetic-act-fdc-act

Forescout Research Labs. (2020). *Connected Medical Device Security: A Deep Dive into Healthcare Networks*. https://www.forescout.com/resources/connected-medical-device-security-a-deep-dive-into-healthcare-networks/

Goldsmith, L. J. (2021). Using Framework Analysis in Applied Qualitative Research. *The Qualitative Report*, *26*(6), 2061–2076. https://doi.org/10.46743/2160-3715/2021.5011

Herrero, L., Sánchez-Santiago, B., Cano, M., Sancibrian, R., Ratwani, R., & Peralta, G. (2023). Prioritizing Patient Safety: Analysis of the Procurement Process of Infusion Pumps in Spain. *International Journal of Environmental Research and Public Health 2023, Vol. 20, Page 7179*, *20*(24), 7179. https://doi.org/10.3390/IJERPH20247179

Hinrichs-Krapels, S., Ditewig, B., Boulding, H., Chalkidou, A., Erskine, J., & Shokraneh, F. (2022). Purchasing high-cost medical devices and equipment in hospitals: a systematic review. *BMJ Open*, *12*(9), e057516. https://doi.org/10.1136/bmjopen-2021-057516

IMDRF. (n.d.). *About IMDRF* . Retrieved April 17, 2024, from https://www.imdrf.org/about

IMDRF Management Committee. (2020). *IMDRF Strategic Plan 2021 - 2025*. https://www.imdrf.org/documents/imdrf-strategic-plan-2021-2025

Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in Hospitals: A Systematic, Organizational Perspective. *J Med Internet Res 2018;20(5):E10059 Https://Www.Jmir.Org/2018/5/E10059*, *20*(5), e10059. https://doi.org/10.2196/10059

Jalali, M. S., Razak, S., Gordon, W., Perakslis, E., & Madnick, S. (2019). Health Care and Cybersecurity: Bibliometric Analysis of the Literature. *J Med Internet Res 2019;21(2):E12644 Https://Www.Jmir.Org/2019/2/E12644*, *21*(2), e12644. https://doi.org/10.2196/12644

Khalil, K. (2023, September 4). *Q&A: The facts about the PATCH Act - Medical Device Network*. https://www.medicaldevice-network.com/interviews/qa-the-facts-about-the-patch-act/?cf-view

Klonoff, D. C. (2015). Cybersecurity for Connected Diabetes Devices. *Journal of Diabetes Science and Technology*, *9*(5), 1143–1147. https://doi.org/10.1177/1932296815583334

Lam, M. L.-L., & Wong, K. W. (2018). Embracing Cybersecurity Risk Management in the Industry of Medical Devices. In *Analyzing the Impacts of Industry 4.0 in Modern Business Environments* (pp. 177–197). IGI Global. https://doi.org/10.4018/978-1-5225-3468-6.ch010

Lechner, N. H. (2017). An overview of cybersecurity regulations and standards for medical device software. *Central European Conference on Information and Intelligent Systems*, 237–249.

Lenz, J., Bozakov, Z., Wendzel, S., & Vrhovec, S. (2023). Why people replace their aging smart devices: A push–pull–mooring perspective. *Computers & Security*, *130*, 103258. https://doi.org/10.1016/J.COSE.2023.103258

Lingg, M., Merida-Herrera, E., Wyss, K., & Durán-Arenas, L. (2017). ATTITUDES OF ORTHOPEDIC SPECIALISTS TOWARD EFFECTS OF MEDICAL DEVICE PURCHASING. *International Journal of Technology Assessment in Health Care*, *33*(1), 46–53. https://doi.org/10.1017/S0266462317000101

Lingg, M., Wyss, K., & Durán-Arenas, L. (2016). Effects of procurement practices on quality of medical device or service received: A qualitative study comparing countries. *BMC Health Services Research*, *16*(1), 1–13. https://doi.org/10.1186/S12913-016-1610-4/TABLES/4

Ludvigsen, K. R. (2023). The Role of Cybersecurity in Medical Devices Regulation: Future Considerations and Solutions. *Law, Technology and Humans*, *5*(2), 59–77. https://doi.org/10.5204/lthj.3080

Martin, T., Guercio, A., Besseau, H., Huot, L., Guerre, P., Atfeh, J., Piazza, L., Pineau, J., Sabatier, B., Borget, I., & Martelli, N. (2023). Hospital-based health technology assessment of innovative medical devices: insights from a nationwide survey in France. *International Journal of Technology Assessment in Health Care*, *39*(1), e58. https://doi.org/10.1017/S0266462323000521

McLeod, A., & Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decision Support Systems*, *108*, 57–68. https://doi.org/10.1016/J.DSS.2018.02.007

MDCG. (2020). *Guidance on Cybersecurity for medical devices*. https://ec.europa.eu/docsroom/documents/41863

Medical Device Cybersecurity Working Group. (2020). *Principles and Practices for Medical Device Cybersecurity*. https://www.imdrf.org/documents/principles-and-practices-medical-device-cybersecurity

MedTech Europe. (2023, October 11). *Market - MedTech Europe - The European Medical Technology in Figures*. https://www.medtecheurope.org/datahub/market/

Miller, F. A., Lehoux, P., Peacock, S., Rac, V. E., Neukomm, J., Barg, C., Bytautas, J. P., & Krahn, M. (2019). How Procurement Judges The Value of Medical Technologies: A Review of Healthcare Tenders. *International Journal of Technology Assessment in Health Care*, *35*(1), 50–55. https://doi.org/10.1017/S0266462318003756

Minaar, A., & Herbig, F. J. W. (2021). Cyberattacks and the cybercrime threat of ransomware to hospitals and healthcare services during the COVID-19 pandemic. *Acta Criminologica: African Journal of Criminology & Victimology*, *34*(3), 155–185.

Ministry of Economic Affairs and Climate Policy. (n.d.-a). *NIS2-startpunt | Digital Trust Center*. Retrieved April 1, 2024, from https://www.digitaltrustcenter.nl/nis2/startpunt

Ministry of Economic Affairs and Climate Policy. (n.d.-b). *Wat is de NIS2-richtlijn? | Digital Trust Center*. Retrieved April 2, 2024, from https://www.digitaltrustcenter.nl/wat-is-de-nis2-richtlijn#bijlage1

Minning, H. (2020). The Reputational Landscape of Medical Device Companies: A Hospital Procurement Manager's Perspective. *Doctoral Thesis, University of Gloucestershire*. https://doi.org/10.46289/BUSM2389

Moon, B. (1995). Paradigms in migration research: Exploring 'moorings' as a schema. *Progress in Human Geography*, *19*(4), 504–524. https://doi.org/10.1177/030913259501900404/ASSET/030913259501900404.FP.PNG_V03

Muittari, M. (2023). *How do Dutch hospitals purchase high-tech medical devices?* [Lappeenranta-Lahti University of Technology & University of Twente]. https://lutpub.lut.fi/bitstream/handle/10024/166037/Masters_Thesis_Manta_Muittari.pdf?sequence=3&isAllowed=y

Nayak, B., Bhattacharyya, S. S., Goswami, S., & Thakre, S. (2022). Adoption of online education channel during the COVID-19 pandemic and associated economic lockdown: an empirical study from push–pull-mooring framework. *Journal of Computers in Education*, *9*(1), 1–23. https://doi.org/10.1007/S40692-021-00193-W/TABLES/6

NEN. (2017). *NEN 7510: Informatiebeveiliging in de zorg* . https://www.nen.nl/zorg-welzijn/ict-in-de-zorg/informatiebeveiliging-in-de-zorg

NVZ, NFU, RN, & ZKN. (2016). *Convenant Veilige Toepassing van Medische Technologie in de medisch specialistische zorg*. https://www.vmszorg.nl/wp-content/uploads/2017/11/Convenant-medische-technologie-tweede-druk-2016.pdf

Nyhlén, J., & Lidén, G. (2014). Methods for analyzing decision-making: A framework approach. *Quality and Quantity*, *48*(5), 2523–2535. https://doi.org/10.1007/S11135-013-9905-6/TABLES/2

Parkinson, S., Eatough, V., Holmes, J., Stapley, E., & Midgley, N. (2016). Framework analysis: a worked example of a study exploring young people's experiences of depression. *Qualitative Research in Psychology*, *13*(2), 109–129. https://doi.org/10.1080/14780887.2015.1119228

PATCH Act of 2022 (2022). https://www.congress.gov/bill/117th-congress/house-bill/7084/text

Ponemon Institute. (2023). *Cyber Insecurity in Healthcare: The Cost and Impact on Patient Safety and Care.* https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-cyber-insecurity-healthcare-ponemon-report.pdf

Pranckutė, R. (2021). Web of Science (WoS) and Scopus: The Titans of Bibliographic Information in Today's Academic World. *Publications*, *9*(1), 12. https://doi.org/10.3390/publications9010012

Prier, E., & Mccue, C. P. (2009). THE IMPLICATIONS OF A MUDDLED DEFINITION OF PUBLIC PROCUREMENT. *JOURNAL OF PUBLIC PROCUREMENT*, *9*(4), 326–370.

Priestman, W., Collins, R., Vigne, H., Sridharan, S., Seamer, L., Bowen, D., & Sebire, N. J. (2019). Lessons learned from a comprehensive electronic patient record procurement process—implications for healthcare organisations. *BMJ Health & Care Informatics*, *26*(1), e000020. https://doi.org/10.1136/BMJHCI-2019-000020

Racchi, M., Govoni, S., Lucchelli, A., Capone, L., & Giovagnoni, E. (2016). Insights into the definition of terms in European medical device regulation. *Expert Review of Medical Devices*, *13*(10), 907–917. https://doi.org/10.1080/17434440.2016.1224644

Rahmani, K., Karimi, S., Raeisi, A. R., & Rezayatmand, R. (2022). Comparative Study of Medical Equipment Procurement in Selected Countries. *Medical Journal of The Islamic Republic of Iran (MJIRI)*, *36*(1), 302–309. https://doi.org/10.47176/MJIRI.36.40

Rahmani, K., Karimi, S., Rezayatmand, R., & Raeisi, A. R. (2021). Value-Based procurement for medical devices: A scoping review. *Medical Journal of the Islamic Republic of Iran*, *35*(1), 1–9. https://doi.org/10.47176/MJIRI.35.134

Ratta, P., Kaur, A., Sharma, S., Shabaz, M., & Dhiman, G. (2021). Application of Blockchain and Internet of Things in Healthcare and Medical Sector: Applications, Challenges, and Future Perspectives. *Journal of Food Quality*, *2021*. https://doi.org/10.1155/2021/7608296

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (2016). http://data.europa.eu/eli/reg/2016/679/oj

Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on Medical Devices, Amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and Repealing Council Directives 90/385/EEC and 93/42/EEC (2023). http://data.europa.eu/eli/reg/2017/745/oj

Rogers, E. (2003). *Diffusion of Innovations* (5th ed.). Simon and Schuster.

Salm, L. van der. (2022). *Challenges in the decision-making process for Dutch healthcare organisations : The purchasers' perspective*. University of Twente.

Schatz, D., Bashroush, R., Wall, J., & V12n2, J. (2017). Towards a More Representative Definition of Cyber Security. *Journal of Digital Forensics, Security and Law*, *12*(2), 8. https://doi.org/https://doi.org/10.15394/jdfsl.2017.1476

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*(2), 103–111. https://doi.org/10.2345/0899-8205-52.2.103

Singh, C. (2023). Review of the Changes Brought In By the Network and Information Security 2 (NIS2) Directive 2022/2555. *International Company and Commercial Law Review*, *5*, 251–261. https://doi.org/10.2872/23955

Turrell, A. (2014). DEVELOPING A PUBLIC VALUE HEALTHCARE PROCUREMENT FRAMEWORK. *JOURNAL OF PUBLIC PROCUREMENT*, *13*, 476–515.

U.S. Department of Health and Human Services. (n.d.-a). *Breach Notification Rule*. Retrieved April 3, 2024, from https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

U.S. Department of Health and Human Services. (n.d.-b). *Summary of the HIPAA Privacy Rule*. Retrieved April 3, 2024, from https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

U.S. Department of Health and Human Services. (n.d.-c). *Summary of the HIPAA Security Rule*. Retrieved April 3, 2024, from https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

Uwizeyemungu, S., Poba-Nzaou, P., & Cantinotti, M. (2019). European Hospitals' Transition Toward Fully Electronic-Based Systems: Do Information Technology Security and Privacy Practices Follow? *JMIR Med Inform 2019;7(1):E11211 Https://Medinform.Jmir.Org/2019/1/E11211*, *7*(1), e11211. https://doi.org/10.2196/11211

Vandezande, N. (2024). Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. *Computer Law & Security Review*, *52*, 105890. https://doi.org/10.1016/J.CLSR.2023.105890

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, *27*(3), 425. https://doi.org/10.2307/30036540

Vincent, C. J., & Blandford, A. (2017). How do health service professionals consider human factors when purchasing interactive medical devices? A qualitative interview study. *Applied Ergonomics*, *59*, 114–122. https://doi.org/10.1016/J.APERGO.2016.08.025

Wee, B. Van, & Banister, D. (2016). How to Write a Literature Review Paper? *Transport Reviews*, *36*(2), 278–288. https://doi.org/10.1080/01441647.2015.1065456

Williams, P. A., Woodward, A. J., williams Andrew J woodward, P. A., & williams, P. A. (2015). Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem. *Medical Devices: Evidence and Research*, *8*, 305–316. https://doi.org/10.2147/MDER.S50048

Yeng, P. K., Wulthusen, S. D., & Yang, B. (2020). Legal Requirements towards Enhancing the Security of Medical Devices. *IJACSA) International Journal of Advanced Computer Science and Applications*, *11*(11). www.ijacsa.thesai.org

Yuan, S., Fernando, A., & Klonoff, D. C. (2018). Standards for Medical Device Cybersecurity in 2018. *Journal of Diabetes Science and Technology*, *12*(4), 743–746. https://doi.org/10.1177/1932296818763634

Zou, X., & Mehta, T. (2023). *5 Ways Hospitals Can Help Improve Their IoT Security*. https://www.darkreading.com/ics-ot-security/5-ways-hospitals-can-help-improve-their-iot-security

Appendix A - Interviews

This appendix provides the documentation used during the conducted interviews.

A.1 Interview protocol for hospital stakeholders

All interviews with hospital stakeholders were held in Dutch. Therefore, the interview protocol is also in Dutch. However, an English translation is provided for readers not fluent in Dutch.

A.1.1 Dutch interview protocol

Dit interviewprotocol is bedoeld om structuur aan te brengen in de semigestructureerde interviews die voor deze scriptie zijn gehouden. Voorafgaand aan dit interview werden de deelnemers geïnformeerd over het doel van het onderzoek en werd hen gevraagd om via e-mail een informed consent te ondertekenen.

Inleiding

Welkom en bedankt voor uw tijd vandaag. Ik begin nu met de opname van dit interview. Als u op enig moment tijdens het interview de opname wilt stoppen, laat het me dan weten. Bedankt voor het ondertekenen van het informed consent via e-mail/fysiek voorafgaand aan dit interview. Het doel van dit interview is om uw ervaring met het inkopen van medische apparatuur binnen uw organisatie in kaart te brengen. Sommige vragen zijn misschien te specifiek voor u om te beantwoorden. In dat geval kunt u dit aangeven en kunnen we bespreken wat u wel weet. Dit interview zal ongeveer 60 minuten duren, dus laten we beginnen.

Achtergrond deelnemer

Voordat we verder ingaan op het aankoopproces, ben ik benieuwd naar je eigen professionele achtergrond en die van de organisatie.

1. Wat is uw rol bij deze organisatie?
    a. Hoe lang vervult u deze functie al?
    b. Kunt u kort uw dagelijkse verantwoordelijkheden binnen deze organisatie beschrijven?
2. Wat is uw rol tijdens het inkoopproces van nieuwe medische apparatuur?
3. Aan hoeveel inkoopprocessen van medische apparatuur heb je bijgedragen?
4. Hoeveel medische apparatuur zijn er in uw organisatie?
    a. Van deze medische apparatuur, hoeveel zijn er verbonden met een IT-netwerk?

Inkoopproces

1. Hoe wordt het inkoopproces van nieuwe medische apparatuur gestart?
    a. Wie start dit proces?
    b. Wat zijn de redenen om een nieuw proces te starten?
    c. Zijn er externe factoren zoals nieuw beleid of een adviesorgaan, die de aanschaf van nieuwe apparatuur motiveren?
2. Welke nationale en internationale regelgeving wordt gevolgd tijdens het inkoopproces van nieuwe medische apparatuur?
3. Hoe worden de eisen vastgesteld waaraan nieuwe medische apparatuur moet voldoen?
    a. Wie zijn hierbij betrokken en welke rol hebben zij in de organisatie?
    b. Hoe worden de eisen verzameld (bijvoorbeeld vergaderingen)?
    c. (Indien nog niet genoemd) Stelt uw ziekenhuis specifieke eisen aan cybersecurity voor medische apparatuur?
        i. Welke eisen zijn dat?
        ii. Welke rollen en departementen bepalen doorgaans deze eisen binnen uw organisatie?
        iii. Hoe worden deze stakeholders vervolgens betrokken bij het prioriteren van deze eisen en het uiteindelijke besluit proces?
        iv. Zijn er specifieke beveiligingsrisico's waar u of uw organisatie zich zorgen over maakt met betrekking tot (verbonden) medische apparatuur?
        v. Worden beveiliging patches voor de apparatuur op de lange termijn overwogen?
        vi. Worden componenten van derden die in medische apparatuur zit in overweging genomen tijdens een mogelijke evaluatie van de cybersecurity?
        vii. Kunt u ingaan op een recente aanschaf van een aangesloten medisch apparaat waarbij cyberbeveiligingseisen in overweging werden genomen? (Om welk apparaat ging het? Wat waren precies de cybervereisten? Hoe werd er onderhandeld tussen de belanghebbenden?)
4. Welke eisen worden over het algemeen gesteld bij het inkopen van nieuwe medische apparatuur?

5. Hoe worden offertes geëvalueerd?
    a. Wie is bij de evaluatie betrokken?
    b. Waar wordt naar gekeken?
    c. Wie heeft het laatste woord bij het selecteren van een offerte?
    d. (Als cybersecurity wordt overwogen door het ziekenhuis) Hoe beoordeelt uw ziekenhuis de cybersecurity van apparatuur?
6. Worden offertes en leveranciers achteraf geëvalueerd?
    a. Hebben eerdere ervaringen met leveranciers invloed op inkoopprocessen?
    b. Hebben eerdere ervaringen met apparatuur invloed op de eisen voor toekomstige apparatuur?

Slotverklaring
Dank u voor uw tijd en deelname. Is er volgens u nog iets belangrijks met betrekking tot het inkoopproces van medische apparatuur of cybersecurity van medische apparatuur dat we nog niet hebben besproken? Nadat ik dit interview heb verwerkt, stuur ik u ter verificatie een samenvatting van mijn bevindingen. Als u geïnteresseerd bent, kan ik ook mijn thesis delen zodra deze is afgerond.

A.1.2 English interview protocol

This interview protocol aims to structure the semi-structured interviews held for this thesis. Prior to this interview, participants were informed on the purpose of the study and were asked to sign an informed consent form via email. Below the interview structure for hospitals is detailed.

Introduction
Welcome and thank you for your time today. I will now start the recording of this interview. If at any time during the interview you would like to stop the recording, please let me know. Thank you for signing the informed consent form via email/physically prior to this interview. The purpose of this interview is to map your experience with procuring interconnected medical devices at your organisation. With interconnected medical devices I mean that the devices are or will be connected to a hospital's IT infrastructure. Some questions might be too specific for you to answer. In that case, feel free to mention this and we can discuss what you do know. This interview will take approximately 60 minutes, so let's start.

Participant background
Before dive into the procurement process, I am curious about your own professional background as well as that of the organization.

1. What is your role at this organization?
    a. How long have you been in this role?
    b. Can you describe your daily responsibilities within this organization?
2. What is your role during the procurement process of new medical devices?
3. How many medical device procurement processes have you contributed to?
4. How many medical devices are there in your organization?
    a. Of these medical devices, how many are interconnected?

Procurement specific
Now let's move to the procurement of medical devices at your organisation.

1. How is a new procurement process for medical devices started?
    a. Who initiates it?
    b. What are the reasons?
    c. Are there any external forces, such as new policies or an advisory body, that motivate the purchase of new medical devices?
2. Which national and international regulations are followed during the procurement of new medical devices?
3. How are requirements set for new medical devices in your organisation?
    a. Who are involved and what roles do they have?
    b. How are the requirements gathered (i.e. meetings?)
    c. Does your hospital put forward specific cybersecurity requirements for medical devices?
        i. If yes, how do these requirements look like?
        ii. Are there any specific security risks you are concerned with when it comes to connected medical devices at your organization?
        iii. (If not mentioned yet) Are long-term security patches considered?

iv. (If not mentioned yet) Are third-party components that are put into the devices considered during a potential cybersecurity evaluation?
v. Which roles and departments usually define the security requirements at your organisation?
vi. How are these stakeholders then involved in the requirement prioritization and procurement process?
vii. Could you elaborate on a recent procurement of a connected medical device where cybersecurity requirements were considered? (Which device was it? What exactly were the cyber requirements? How was it negotiated across stakeholders?

4. Could you elaborate on the general requirements of a recent procurement process you contributed to?
5. How are offers evaluated?
   a. Who evaluates them?
   b. What do they look for?
   c. Who has the final say when it comes to selecting an offer?
   d. In your experience, how are security requirements factored into the final decision?
   e. (If cybersecurity is considered by hospitals) How does your hospital assess the cybersecurity of devices?
6. Are offers and their performance evaluated afterwards?
   a. Do previous experiences with suppliers influence future procurement processes?
   b. Do previous experiences with devices influence the requirement for future procurement processes?

Closing statement

Thank you for your time and participation. Is there in your view anything else important regarding the procurement process of medical devices or cybersecurity of medical devices that we haven’t discussed yet? After I have processed this interview, I will send you a summary of my findings to verify them. If you are interested, I can also share my thesis once completed.

A.2 Interview protocol for external stakeholders

A different interview protocol was drafted for external stakeholders that might be related to the procurement process within hospitals. Interviews were held in Dutch; therefore, the interview protocol is also in Dutch. For readers not proficient in Dutch, an English translation is provided.

A.2.1 Dutch interview protocol

Dit interviewprotocol is bedoeld om structuur aan te brengen in de semigestructureerde interviews die voor deze scriptie zijn gehouden. Voorafgaand aan dit interview werden de deelnemers geïnformeerd over het doel van het onderzoek en werd hen gevraagd om via e-mail een informed consent te ondertekenen.

Inleiding

Welkom en bedankt voor uw tijd vandaag. Ik begin nu met de opname van dit interview. Als u op enig moment tijdens het interview de opname wilt stoppen, laat het me dan weten. Ik wil u ook bedanken voor het ondertekenen van het informed consent via e-mail/fysiek voorafgaand aan dit interview. Het doel van dit interview is om de invloed van uw organisatie op het inkoopproces van verbonden medische apparatuur in ziekenhuizen in kaart te brengen. Met verbonden medische apparatuur bedoel ik dat het apparaat wordt aangesloten op het IT-netwerk van een ziekenhuis. Sommige vragen zijn misschien te specifiek voor u om te beantwoorden. In dat geval kunt u dit aangeven en kunnen we bespreken wat u wel weet. Dit interview zal ongeveer 30 minuten duren, dus laten we beginnen.

Achtergrond deelnemer

Voordat we in de inkoopprocessen en jouw organisatie duiken, ben ik benieuwd naar je eigen professionele achtergrond.

1. Wat is uw rol bij deze organisatie?
   a. Hoe lang vervult u deze functie al?
   b. Kunt u uw dagelijkse verantwoordelijkheden binnen deze organisatie beschrijven?
2. Heb je ervaring met cybersecurity in ziekenhuizen?
3. Wat voor rol speelt uw organisatie met betrekking tot de inkoop van medische apparatuur in ziekenhuizen en cybersecurity?

Inkoopproces

Laten we nu overgaan op de inkoop van medische apparatuur in ziekenhuizen.

1. Heeft uw organisatie een officieel advies/beleid als het gaat om de inkoop van medische apparatuur in ziekenhuizen?
   a. Zo ja, wat houdt dit in?
   b. Hoe wordt gedeeld/gehandhaafd met ziekenhuizen?
2. Is uw organisatie wel eens actief betrokken bij de aanschaf van nieuwe, verbonden, medische apparatuur in ziekenhuizen?
   a. Zo ja, hoe ziet dit eruit?
   b. Zo nee, vindt u dat dit zou moeten?
3. Wat zijn volgens uw organisatie de dingen die ziekenhuizen zouden moeten overwegen tijdens het inkoopproces van nieuwe medische apparatuur?

Apparaat beveiliging

De volgende vragen zijn gespecificeerd naar de cybersecurity van medische apparatuur.

1. Heeft uw organisatie een officieel advies of beleid voor cybersecurity van medische apparatuur?
   a. Zo ja, wat houdt dit in?
   b. Hoe wordt dit gedeeld/gehandhaafd met ziekenhuizen?
   c. Hoe wordt het gedeeld/gehandhaafd met fabrikanten?
2. Hoe kan de cybersecurity in ziekenhuizen volgens u worden verbeterd?
   a. Is dit iets dat actief wordt gecommuniceerd?

Slotverklaring

Dank u voor uw tijd en deelname. Is er volgens u nog iets belangrijks met betrekking tot het inkoopproces van medische apparatuur of cybersecurity van medische apparatuur dat we nog niet hebben besproken? Nadat ik dit interview heb verwerkt, stuur ik u ter verificatie een samenvatting van mijn bevindingen. Als u geïnteresseerd bent, kan ik ook mijn scriptie delen zodra deze is afgerond.

A.2.2 English interview protocol

This interview protocol aims to structure the semi-structured interviews held for this thesis. Prior to this interview, participants were informed on the purpose of the study and were asked to sing an informed consent form via email.

Introduction

Welcome and thank you for your time today. I will now start the recording of this interview. If at any time during the interview you would like to stop the recording, please let me know. I would also like to thank you for signing the informed consent form via email/physically prior to this interview. The purpose of this interview is to map your organisation's influence on the procurement process of interconnected medical devices in hospitals. With interconnected medical devices I mean that the devices are or will be connected to a hospital's IT infrastructure. Some questions might be too specific for you to answer. In that case, feel free to mention this and we can discuss what you do know. This interview will take approximately 30 minutes, so let's start.

Participant background:

Before we dive into the procurement processes and your organisation, I am curious about your own professional background.

1. What is your role at this organization?
    a. How long have you been in this role?
    b. Can you describe your daily responsibilities within this organization?
2. Do you have experience with cybersecurity in hospitals?
3. What is the responsibility of your organisation on the topic of procurement and cybersecurity?

Procurement specific:

Now let's move to the procurement of medical devices in hospitals.

1. Does your organization have any official advice / policy when it comes to procurement of medical devices in hospitals?
    a. If yes, what does it entail?
    b. How is it shared / enforced with hospitals?
2. Is your organization ever actively involved in the procurement of new medical devices in hospitals?
    a. If yes, how does this look like?
    b. If not, do you think it should?
3. In the view of your organization, what are the things that a hospital should consider during the procurement of new medical devices?

Device specific cybersecurity:

The following questions are specified to the cybersecurity of medical devices.

1. Does your organization have any official advice / policy for connected medical device cybersecurity?
    a. If yes, what does it entail?
    b. How is it shared / enforced with hospitals?
    c. How is it shared / enforced with manufacturers?
2. How could cybersecurity practices be improved at hospitals in your view?
    a. Is this something that is actively communicated?

Closing statement

Thank you for your time and participation. Is there in your view anything else important regarding the procurement process of medical devices or cybersecurity of medical devices that we haven't discussed yet? After I have processed this interview, I will send you a summary of my findings to verify them. If you are interested, I can also share my thesis once completed.

A.3 Informed consent

As previously mentioned, all interviews were conducted in Dutch. In order to make sure that the participants fully understood the informed consent, they were also provided with a Dutch informed consent form. However, an English translation is provided for readers not fluent in Dutch.

A.3.1 Dutch informed consent

U wordt uitgenodigd om deel te nemen aan een onderzoek genaamd Security and Safety in Hospital Procurement Processes in the Netherlands. Dit onderzoek wordt uitgevoerd door Ewoud Cornelissen van de TU Delft en wordt begeleid door Dr. Rolf van Wegberg. Dit onderzoek is ter afronding van mijn Masteropleiding Complex Systems Engineering and Management aan de TU Delft.

Het doel van dit onderzoek is om de rol van veiligheid tijdens het inkoopproces van nieuwe medische apparatuur in Nederlandse ziekenhuizen en de blik die verschillende stakeholders hierop hebben in kaart te brengen. Dit interview zal ongeveer 60 minuten in beslag nemen.

U wordt gevraagd naar uw ervaringen en visie op het inkoop- en implementatieproces van nieuwe medische apparatuur in Nederlandse ziekenhuizen. De resultaten van dit interview zullen worden gebruikt voor mijn masterscriptie en eventuele wetenschappelijke publicatie daarna.

Zoals bij elk interview is het risico van een databreuk aanwezig. Wij doen ons best om uw antwoorden vertrouwelijk te houden. We minimaliseren de risico's door de verzameling van informatie op basis waarvan u als uniek individu kunt worden geïdentificeerd, tot een minimum te beperken. Gegevens die worden verzameld zijn: uw algemene functieomschrijving (bijv. 'Medisch medewerker, 'IT-medewerker'), omvang van het ziekenhuis in termen van aantal bedden (bijv. 200 - 499). Alle andere informatie aan de hand waarvan u uniek geïdentificeerd zou kunnen worden, wordt niet gedeeld en wordt aan het einde van dit project vernietigd.

De audio van dit interview zal worden opgenomen en in tekstformaat worden getranscribeerd. Het schriftelijke transcript van dit interview wordt geanonimiseerd door alle informatie te verwijderen waarmee u, of uw organisatie uniek geïdentificeerd zou kunnen worden. De audio-opname en dit ondertekende Informed Consent formulier worden uitsluitend opgeslagen op TU Delft's OneDrive en worden met niemand anders gedeeld dan met de Thesis committee die dit onderzoek begeleidt. Het transcript kan worden gebruikt voor toekomstige onderzoeks- en onderwijsactiviteiten van de Thesis committee over het onderwerp van (digitale) veligheid in het domein van de gezondheidszorg. U zult in dergelijk gebruik geheel anoniem blijven. Alle data zal uiterlijk 15/08/2025 worden verwijderd na het afronden van het PhD project van Lorenz Kustosch, lid van het Thesis committee.

Uw deelname aan dit onderzoek is volledig vrijwillig, en u kunt zich elk moment terugtrekken zonder reden op te geven. U bent vrij om vragen niet te beantwoorden. Indien u zich terugtrekt vóór het einde van dit master thesis project (01/07/2024), dan worden uw gegevens verwijderd en niet gebruikt.

Graag vraag ik u dit document te ondertekenen als u akkoord bent met het bovenstaande. Mochten er nog onduidelijkheden of vragen zijn, neem dan gerust contact met mij op via e.r.w.cornelissen@student.tudelft.nl
Na 1 september 2024 kunt u contact opnemen met Lorenz Kustosch via l.f.kustosch@tudelft.nl

Handtekening

____________________________ ____________________________ ________
Naam deelnemer Handtekening Datum

A.3.2 English informed consent

You are being invited to participate in a research study titled Security and Safety in Hospital Procurement Processes in the Netherlands. This study is being done by Ewoud Cornelissen, Master student at the TU Delft for my thesis for the Master Complex Systems Engineering and Management. This thesis is supervised by Dr. Rolf van Wegberg.

The purpose of this research study is to understand the role of security and safety during the procurement of new medical devices in Dutch hospitals and the view different involved stakeholders have on this. This interview will take approximately 60 minutes.

In this interview I will ask you about your experiences and view on the procurement and implementation process of new medical devices in Dutch hospitals. The results of this interview will be used for my Master thesis and potential scientific publication afterwards.

As with any interview the risk of a breach is always possible. To the best of our ability your answers in this study will remain confidential. We will minimize any risks by minimizing the collection of information on which you could be uniquely identified as an individual. Data that will be collected is: your general job description (e.g. 'Medical staff member, 'IT staff member'), hospital size range by means of number of beds (e.g. 200-499). All other information on which you could be uniquely identified will not be shared and will be destroyed at the end of this project.

The interview will be audio recorded and transcribed into text format. The written transcript of this interview will be anonymized by removing all information on which you, or your organization could be uniquely identified. This includes anything that might come up during the interview. The audio recording and this signed consent form will solely be stored on TU Delft' OneDrive and will not be shared with anyone else besides the Thesis committee guiding this research. The transcript can be used for future research and educational activities by the Thesis committee, on the topic of security and safety in the domain of healthcare - you will not be identifiable in such output. All data will be destroyed on 15/08/2025 the latest in accordance with the PhD project of Lorenz Kustosch, member of the Thesis committee.

Your participation in this study is entirely voluntary and you can withdraw at any time. You are free to omit any questions. If you withdraw before the end of this Master thesis project (01/07/2024), your data will be deleted and not used.

Please sign this document if you agree with the aforementioned.
If any questions or remarks remain, please contact the researcher at e.r.w.cornelissen@student.tudelft.nl up to September 1st 2024. Afterwards, please contact Lorenz Kustosch at l.f.kustosch@tudelft.nl

Signature

______________________________	____________________________	_________
Name of participant [printed]	Signature	Date

Appendix B – MDR requirements

The table below depicts all cybersecurity requirements required for medical devices by the MDR, as mentioned in Annex I (Regulation (EU) 2017/745, 2023). The requirements apply to the manufacturer, integrator, and operator. All requirements in regular font are the minimum IT security requirements, whilst the requirements in italic font are best practices as proposed by MDCG (2020).

Table 20 - MDR cybersecurity requirements, adapted from MDCG (2020)

Req. num.	*Requirement description*
Part 1: Governance and Ecosystem	
1.1	*Perform risk and impact assessment in accordance with industry standards for medical devices.*
1.2	Have an adequate patch management process in place that is deployed in a timely manner for medical devices and the operating environment.
1.3	Solely use genuine software and ban all illegitimate software.
1.4	*Define a set of minimum IT security policies which are approved by management.*
	1.4.1 *Define clear roles for users of critical medical devices and systems and segregate duties.*
	1.4.2 *Define information classification levels and label devices handling such information accordingly.*
	1.4.3 *Implement an acceptable use policy and a change management policy.*
	1.4.4 *Establish a backup policy on the selected critical systems.*
	1.4.5 *Establish a procurement policy for provisioning new medical devices*
	1.4.6 *Include detailed SLAs and NDAs to manufacturers and third parties.*
1.5	*Policies should be communicated to employees and third parties.*
1.6	*Have security awareness trainings for users that operate critical devices and systems.*
1.7	*Perform background checks prior to authorizing users to access medical devices and systems.*
1.8	*Index medical devices and other relevant assets in inventory. Assign unique IDs to systems and medical devices.*
Part 2: Protection	
2.1	Operating environment must not hinder the application of security measures on the medical device or force the device to operate in lower security settings.
2.2	The system should include session management measures (e.g. session timeouts).
2.3	The system should include operating system hardening and application whitelisting.
2.4	The system should have antivirus / anti-malware software.
2.5	The system should have strong passwords.
2.6	*The systems should have appropriate security measures for mobile devices and teleworking.*
2.7	The system should use a firewall.
2.8	The system should use network segmentation.
2.9	The system should use partitioning mechanisms and traffic segmentation.
2.10	The system should use traffic filtering software and hardware.
2.11	The system should use encryption when storing sensitive personal data.
2.12	The system should use encryption when data is in transit.
2.13	The system should have memory protection measures to block arbitrary code execution.
2.14	The system should have compatibility of medical device management software with security solutions that counter malicious code.
2.15	The systems should only have software programmes installed necessary for the intended uses.
2.16	The system should use user access management .
2.17	*Apply the principle of least privilege to user workstations and connected devices.*

2.18	*Least privileges must take into account data minimisation per role.*
2.19	Provisions should be in place regarding patch management.
2.20	Support patching without compromising interoperability and compatibility.
2.21	*Do not use end-of-life third-party components and devices on the operating environment.*
2.22	Regulated and authenticated physical access measures should be in place via suitable technical measures (e.g. badges).
2.23	Define roles and access rights, including those for physical access to medical devices.
2.24	Make use of segregated, secure areas with appropriate access controls.
Part 3: Defence	
3.1	Implement software integrity checks and device authentication.
3.2	*Data integrity should be ensured through, for example, hashing or integrity checks.*
3.3	*Monitor and keep track of changes in ecosystem parties, so that the business processes are not interrupted or hide risks.*
3.4	*The Health Information System (HIS) must be able to monitor the correct operation of the equipment in the context of medical workflows.*
Part 4: Resilience	
4.1	*Investigate major incidents and review actions taken to mitigate and reduce time to react to future occurrences.*
4.2	*Develop a disaster recovery plan, taking into account the minimum recovery requirements.*
4.3	*Implement data recovery mechanisms to critical systems.*

Appendix C – Codebook

This appendix provides the codebook created during the coding process of both the internal and external stakeholder interviews.

C.1 Internal stakeholders codebook

Below, Table 21 provides the codebook of the internal stakeholder interviews. Besides the meaning, the table also provides an overview of any potential link of a sub-code to another theme and shows the number of quotes from the interview transcripts linked to each theme and sub-code.

Table 21 - Internal stakeholder codebook

Theme	*Sub-code*	*Linked to*	*# quotes*	*Meaning*
Stakeholders		None	50	All stakeholders involved in the procurement process.
	Clinical physics	Procurement initiation	7	Clinical physicist working in the hospital.
	Contract manager	None	2	Contract manager that works in the hospital.
	Department head	None	16	The head of a certain hospital department, such as the radiology department.
	Doctors	None	9	Doctors working in the hospital.
	Financial manager	None	4	Someone who is responsible for the finances in a hospital.
	Infection prevention	None	3	Infection prevention specialist working in the hospital.
	IT department	Procurement initiation	12	The IT department of a hospital.
	Medical technology department	Procurement initiation	8	The MedTech department of a hospital.
	Nurses	None	1	Nurses in a hospital.
	Procurement department	None	7	The procurement department of a hospital, internal or external.
Procurement initiation		None	42	Reasons to initiate a procurement process.
	'Owner' of medical device	None	10	The person who is responsible for a medical device in a hospital.
	Dissatisfaction with medical devices	None	3	Dissatisfaction of the current medical device in use.
	End-of-life of medical device	None	13	A medical device who is at the end of its lifecycle.
	Guidelines	Regulations	6	Guidelines from either the NZa or medical specialist associations on medical treatments.
	Hospital rivalry	Outside influences	1	Rivalry with other hospitals to offer the best care possible.
	New medical treatment	None	3	A new treatment for patients that requires a new device.
	New technology on the market	None	13	New technology for medical devices on the market that can improve current treatments given.
Procurement process		None	106	Different steps taken and considerations made during the procurement process.
	Business case and financial check	None	14	A business case is presented to show why a device should be procured and funds are allocated.

Theme	*Sub-code*	*Linked to*	*# quotes*	*Meaning*
	Clear division of roles	None	7	There is clear division of who does what during the procurement process.
	Collaboration with other hospitals	None	7	During the procurement process there is a collaboration with other hospitals.
	Complex process	None	9	Participants mention that the procurement process is complex due to the many steps taken and stakeholders involved.
	Contract negotiation	None	5	Contracts are negotiated with the manufacturer.
	Device on trial	None	6	Before the final decision is made, devices could be installed on a trial basis.
	Discrepancy between stakeholders	None	7	A discrepancy between the stakeholders involved in the procurement process.
	Evaluation	None	8	The procurement process or the suppliers are evaluated.
	Final decision in consultation	None	12	The final decision on which device is procured is made in consultation with all relevant internal stakeholders.
	Market exploration	None	4	The market is explored to see what devices are on offer.
	Offer request and evaluation	None	13	Manufacturers are requested to submit an offer, which is evaluated by the hospital.
	Program of requirements	None	16	A program of requirements is set up.
	Steering committee	None	2	A committee that oversees the procurement process.
	Value threshold	None	5	A threshold after which other procurement process steps are followed.
Requirements		None	94	Requirements set by the hospital for medical devices.
	Aftersales	None	12	The aftersales services provided by manufacturers.
	Cleanability	None	4	How devices can be cleaned.
	Compatibility with other systems	None	5	Compatibility of the device with the (IT) systems already in place in the hospital.
	Cybersecurity	None	29	Cybersecurity requirements set for medical devices and software.
	Data security	None	14	Data security requirements set for medical devices and software.
	Price	None	9	The price of a medical device.
	Regulation compliance	Regulations	10	Whether devices comply with the relevant regulations.
	Reliability	None	3	The reliability and quality of a medical device.
	Repairability	None	6	How devices can be repaired and availability of spare parts.
	Safety	None	6	The safety of a medical device when it is in operation.
	Supplier satisfaction	None	14	How satisfied a hospital is with a certain supplier.
Outside influences		None	15	External influences on the procurement process.

Theme	*Sub-code*	*Linked to*	*# quotes*	*Meaning*
	Manufacturers	None	11	Manufacturers that try to influence a procurement process.
	Medical conference	None	2	Medical conferences where both other doctors and manufacturers are present.
	Other doctors	None	3	Doctors from other hospitals that might influence the doctors involved in the procurement process.
Regulations		None	16	Regulations mentioned by participants.
	Convenant medische technologie	None	2	A sector guideline for medical technology.
	GDPR	None	2	The GDPR is followed by hospitals.
	MDR	None	3	The MDR that manufacturers need to follow for their devices.
	Medical specialists association	Procurement initiation	3	An association for medical specialists that dictate new guidelines.
	NEN7510	None	5	The NEN7510 norm for information security in healthcare.
	Not tender compliant	None	2	Non-academic hospitals are not tender compliant
	NZa	Procurement initiation	2	The Dutch health authority called NZa.
Other		None	9	Other interesting things mentioned by participants.
	No acquisition after procurement process	None	1	Not all procurement processes that are started result in the acquisition of a new device.
	Not cybersecure	None	3	The notion that something was or is not cybersecure.
	Shift to connected medical devices	None	7	A shift is noticeable from regular devices to connected medical devices.

C.2 External stakeholders codebook

Below, Table 22 provides the same overview of the codebook as Table 21, but then specified to the external stakeholder interview.

Table 22 - External stakeholder codebook

Theme	*Sub-code*	*Linked to*	*# quotes*	*Meaning*
Organisational activities		None	11	The activities done by the interviewed organisation.
	Contact with IT specialists mostly	None	2	They mostly have contact with IT specialists from hospitals.
	Give security advice	None	4	They give security advice when requested.
	Proactive scan of vulnerabilities	None	1	The proactively scan their clients on possible vulnerabilities in their IT.
	Share experiences	None	3	Experiences of one client are shared with the other to learn from each other.
	Sole focus on HDOs	None	1	There is only a focus on HDOs, not on manufacturers.
Procurement experiences		None	8	Experiences of the cybersecurity specialists with the procurement process in hospitals.

	Add cybersecurity after procurement	None	1	Cybersecurity is often ‘added’ to the advice after it has been procured.
	Advice for cybersecurity procurement	None	1	They actively advice when cybersecurity measures are procured in hospitals.
	Different views on cybersecurity	None	1	They notice a discrepancy between stakeholders on the importance of cybersecurity.
	Foreign hardware	None	1	Risks associated with foreign hardware are considered.
	Little choice	None	1	There is little choice for hospitals to choose between manufacturers.
	No official procurement advice	None	2	They provide no official cybersecurity advice for procuring medical devices.
	Priority to work efficiency	None	1	They notice a priority in hospitals for work efficiency over cybersecurity.
Sector developments		None	5	Developments noticed in the healthcare sector.
	Regulations improve cybersecurity	None	3	Medical device regulations have improved device cybersecurity over the last couple of years.
	Staff training	None	2	Cybersecurity awareness training should be provided to hospital staff.

Appendix D – Full framework analysis

This appendix includes the full framework analysis table of all hospitals that participated.

Table 23 - Full framework analysis

Theme	*Sub-code*	*H1*	*H2*	*H3*
Stakeholders	*Clinical physics*	The clinical physics department can initiate a procurement process. Additionally, they check the safety and radiation of new devices and contribute to the program of requirements based on their expertise. Finally, they evaluate the servicing agreement with the manufacturer.	The clinical physics department can initiate a procurement process. Additionally, they check the safety and radiation of new devices and contribute to the program of requirements based on their expertise. Finally, they can be a part of the investment committee.	Clinical physicists check the safety and radiation of new devices and contribute to the program of requirements based on their expertise. They can also be part of the investment committee.
	Contract manager	The contract manager evaluates and monitors KPI's agreed with the manufacturer.	The contract manager periodically holds two-way evaluations with suppliers and is part of the MedTech department.	Not mentioned.
	Department head	The department head is the owner of the medical devices on a department. From this position the head can initiate a new procurement process and has a budgetary overview.	The department head is the manager of a specific hospital department. They can start the procurement process of new devices and will have the responsibility to take the lead. They can also be a part of the investment committee.	The department head is the manager of a specific hospital department. They can start a new procurement process based on the end-of-life of a device on the department or based on wishes of the doctors. The head is also responsible to manage the process.
	Doctors	Doctors can initiate a procurement process when they think they need a new device and set requirements for the device to adhere to.	Doctors can initiate a new procurement process. They can also be a part of the investment committee.	Doctors are asked for input during the procurement process based on their expertise.
	Financial manager	The financial manager is responsible for the allocation of funds.	Someone from the finance department is a part of the investment committee.	The investment committee evaluates where money is spent.
	Infection prevention	Infection prevention evaluates the cleanability of devices and can contribute to the program of requirements.	Infection prevention evaluates the cleanability of devices and can contribute to the program of requirements.	Infection prevention evaluates the cleanability of devices and can contribute to the program of requirements.
	IT department	Can initiate the procurement process when required. Contributes to the program of requirements and evaluates cybersecurity measures.	When an IT component is involved in the procurement process, the IT department contributes to the program of requirements. They can also be a part of the investment committee. Is a conjunct department with medical technology. They can	Contributes to the program of requirements and evaluates cybersecurity measures within devices.

Theme	*Sub-code*	*H1*	*H2*	*H3*
			evaluate the cybersecurity of a device.	
	Medical technology department	The medical technology department evaluates the reliability and the serviceability of medical devices.	The medical technology department evaluates the reliability and the serviceability of medical devices. Is a conjunct department with IT.	Can initiate a procurement process when they think a device should be replaced. Contributes to the program of requirements.
	Nurses	The nursing department can contribute to the program of requirements.	Not mentioned.	Not mentioned.
	Procurement department	Has contact with the manufacturers / suppliers. Evaluates the commercial aspect of an offer. Ensures timely renewal of contracts.	The procurement department has to be involved in the process. They give advice based on the total costs of ownership of an offer, including any potential repair costs, and have contact with the manufacturers.	The procurement department is outsourced to a secondary organisation. They have contact with the manufacturers.
Procurement initiation	*Clinical physics*	The clinical physics department might start a new procurement process when they think it is needed.	The clinical physics department might start a new procurement process when they think it is needed.	Not mentioned.
	IT Department	The IT department might start new procurement processes when, for example, the hospital needs to adhere to new regulations.	Not mentioned.	Not mentioned.
	MedTech department	The medical technology department might start a new procurement process when they think it is needed.	Not mentioned.	The medical technology department can start a new procurement process when they think a device should be replaced.
	'Owner' of medical device	Has the main responsibility to guide the procurement process and can initiate the procurement process when new devices are needed.	The owner of the medical device can start a new procurement process when they think the new device is needed.	The owner of the medical device has the leading role in the start of the procurement process.
	Dissatisfaction with medical devices	Dissatisfaction with the current device in use can be the cause to start a new procurement process.	Dissatisfaction with the current device in use can be the cause to start a new procurement process and lead to new requirements for the new device to be procured.	Dissatisfaction with the current device in use can be the cause to start a new procurement process. However, medical devices would still have to be somewhat at the end of their lifecycle before they are allowed to be replaced.
	End-of-life of medical device	When the end of the device's lifecycle is near, a new procurement process to replace it is started. This also	When the end of the device's lifecycle is near, a new procurement process to replace it is started.	When the end of the device's lifecycle is near, a new procurement process to replace it is started.

Theme	*Sub-code*	*H1*	*H2*	*H3*
		holds true for contracts that are about to end.		
	Guidelines	New guidelines from the NZa and medical specialist association can be the cause to procure new devices, if hospitals want to be able to offer certain treatments.	Not mentioned.	New guidelines can force hospitals to replace their devices if they want to offer certain treatments, that their current devices cannot offer.
	Hospital rivalry	Doctors amongst each other can boast about their new devices, which might affect other doctors to procure new devices too in order to remain an attractive hospital.	Not mentioned.	Not mentioned.
	New medical treatment	New medical treatments may need new devices, which can initiate the procurement process.	When a new treatment arises that is more pleasant for the patient, it might be a reason to start the procurement process.	New medical treatments may need new devices, which can initiate the procurement process.
	New technology on the market	New technologies that can improve the treatments offered at the hospital might be the reason to procure new devices.	New technologies that can improve the treatments offered at the hospital might be the reason to procure new devices.	New technologies that can improve the treatments offered at the hospital and which the current devices cannot offer might be the reason to procure new devices. Additionally, new technologies that can improve the work efficiency might be considered.
Procurement process	*Business case and financial check*	Before devices can be procured, funds need to be allocated. Often more funds are requested than available. In that case some persuasion might be needed to prioritise a certain request.	Before devices can be procured, funds need to be allocated. Employees can put in a request with the investment committee to be awarded funds based on a business case they present for the device they want to procure. This should include a medical reasoning and a cost projection.	Before devices can be procured, funds need to be allocated. Employees can put in a request with the investment committee to be awarded funds for the next year based on a business case they present for the device they want to procure.
	Clear division of roles	Within the procurement process a clear division of roles is made. For example, the procurement department is the only department to discuss the offers with manufacturers.	Within the procurement process a clear division of roles is made. For example, everyone that contributes to the program of requirements solely adds and evaluates requirements based on their expertise and role. An exception to this is the MedTech and IT department which are collaborating more and more.	Within the procurement process a clear division of roles is made. For example, everyone that contributes to the program of requirements solely adds and evaluates requirements based on their expertise and role.

Theme	*Sub-code*	*H1*	*H2*	*H3*
	Collaboration with other hospitals	The procurement department and processes are shared with another hospital to drive costs down. However, this does not mean that devices are always installed at the same time. The devices could be bought for the two hospitals, but one hospital will only receive them in two years.	There is no collaboration when buying new devices. However, there is collaboration with other hospitals under the same umbrella organisation on more generic things, such as HR software.	The procurement department is outsourced to a secondary organisation that runs the procurement department of multiple hospitals. This allows them to buy devices in a larger quantity and drive costs down. Additionally, sometimes devices or software are procured together with other hospitals to allow for easier patient transfer between the hospitals.
	Complex process	The process involves a lot of different stakeholders that need to be managed and a lot of different steps.	Procurement projects can be multi-disciplinary and therefore require the expertise of many stakeholders that all need to collaborate.	The process involves a lot of different stakeholders that need to be managed and a lot of different steps.
	Contract negotiation	Part of the process is to negotiate about the contract that includes repair services and technical support.	Part of the process is to negotiate about the contract that includes software updates and aftersales. A standard agreement by WIBAZ is used.	The hospital might negotiate a long-term contract with a supplier that for an extended period of time supplies multiple different devices to the hospital.
	Device on trial	Sometimes devices will be used in the hospital on a trial basis to get a feel with them before they are procured.	Sometimes devices will be used in the hospital on a trial basis before it is procured. If the device is too big, a visit to another hospital that already has the device installed might happen.	Sometimes devices will be used in the hospital on a trial basis under the guidance of the manufacturer to get a feel with them before they are procured.
	Discrepancy between stakeholders	Not mentioned.	The wishes of one stakeholder group can interfere with the wishes of another stakeholder group. For example, the cybersecurity wishes can be too stringent for the medical staff to efficiently do their job.	The wishes of one stakeholder group can interfere with the wishes of another stakeholder group. For example, the cybersecurity wishes can be too stringent for the medical staff to efficiently do their job. Additionally, the MedTech department could say a certain device should already be replaced, whilst the medical staff would prefer to replace another device and there is no budget for both.
	Evaluation	Supplier satisfaction and adherence to previous contracts is taken into account during the procurement process.	The procurement process is evaluated afterwards. Especially when the process did not go as they would have liked. During long	Supplier satisfaction is taken into account when a new procurement process is started. Additionally, regular feedback sessions could be

Theme	*Sub-code*	*H1*	*H2*	*H3*
		However, only the evaluation of the contract is a formal process.	procurement processes, evaluations might even be held during the process to remind everyone on the current status of the process. Supplier satisfaction is taken into account when a new procurement process is started.	scheduled with the manufacturer.
	Final decision in consultation	The final decision for a device is made in consultation with all the different stakeholders involved in the process.	The final decision for a device is made in consultation with all the different stakeholders involved in the process.	The final decision for a device is made in consultation with all the different stakeholders involved in the process.
	Market exploration	Before offer requests are made, a market exploration is performed to map what is on offer.	Market exploration needs to be done before the business case.	Market exploration is done by the external procurement department that sends out offer requests to manufacturers.
	Offer request and evaluation	Once a program of requirements is drafted, offers are requested from manufacturers. If the total amount will be above a certain threshold, at least three offers need to be requested. Offers are evaluated by all participating stakeholders.	Offer requests are coordinated by the external procurement department. Once they receive offers back, they are evaluated by the hospital stakeholders that contributed to the program of requirements.	Offer requests are coordinated by the external procurement department. Once they receive offers back, they are evaluated by the hospital stakeholders that contributed to the program of requirements.
	Program of requirements	A program of requirements is drafted by different stakeholders from within the hospital, such as doctors, infection prevention and IT. These requirements can be completely new, for example when a new technology is introduced, but can also be mostly the same as the previous procurement process.	A program of requirements is drafted by different stakeholders from within the hospital, such as doctors, infection prevention and IT. They do this based on an Excel that is used for all procurement processes in the hospital.	A program of requirements is drafted by different stakeholders from within the hospital, such as doctors, infection prevention and IT. They do this based on a standard format that is used for all procurement processes in the hospital.
	Steering committee	The steering committee consists of the department head, and other relevant stakeholders and are the issuer of the procurement request.	Not mentioned.	Not mentioned.
	Value threshold	Above a couple of thousand euros, at least three offers need to be requested to allow for comparison.	For smaller procurement requests, a separate, bit more informal process is started.	Not mentioned.
Require ments	*Aftersales*	The aftersales services provided by the	Aftersales are considered, such as the supply of spare	Aftersales are considered, such as the supply of spare

Theme	*Sub-code*	*H1*	*H2*	*H3*
		manufacturer, which include: the supply of spare parts, technical assistance availability, servicing.	parts, technical training, and servicing.	parts, technical training, and servicing. Updates are not always considered.
	Cleanability	How devices can be cleaned. For example, if they can withstand 70% alcohol.	If devices make use of disposables.	How devices can be cleaned. For example, if they can withstand 70% alcohol.
	Compatibility with other systems	If devices are compatible with other hospital systems, such as electronic health records.	The device should be able to run on the hospital's network, but should also physically work with other systems, such as operation rooms.	The devices should be able to run on the hospital's network and all software should be able to run on virtual servers.
	Cybersecurity	If the device procured first within the cybersecurity view and accepted risks of the hospital. Compatibility with anti-virus software. Analysis of data being transmitted.	Close attention is paid to devices that support remote access. The preference lies on isolating devices so that they only operate within the safe hospital network. Updates are considered. Devices are analyses on how they work and what possible vulnerabilities they have.	Virus scanners should always be present and up to date. Operating systems should not be x number of versions behind the newest version. Devices are analysed on how they work.
	Data security	Data must be stored in the EU in case the device comes with a SaaS solution. Analysis of data being transmitted.	Patient data should be encrypted.	Data security is a top priority. All data remains within the hospital and is preferably not shared with third parties. If this does happen, stringent agreements are made.
	Price	The maximum funds for the procurement of new devices.	The price includes the total cost of ownership. During contract negotiations, discounts may be requested.	Budget is tight within hospitals, so a close look is always on the price.
	Regulation compliance	Whether devices adhere to relevant regulations, norms, and certifications such as the MDR, NEN7510, ISO, and CE mark.	All devices should adhere to the relevant regulations. If they comply is actively checked.	All devices should adhere to the relevant regulations. Which regulations these are is checked before offers are requested. If the devices comply to these regulations is actively checked.
	Reliability	How reliable devices are and how they withstand rigorous cleaning sessions. Reliability experiences might be checked with other hospitals.	The quality of devices should be up to standards. This can include, for example, the quality of the images the device returns.	The quality of devices should be up to standards. This can include, for example, the quality of the images the device returns.
	Repairability	How easy it is to repair the device yourself, and the availability of spare parts.	How devices can be repaired, availability of spare parts and service agreements with suppliers.	The MedTech department wants to know how devices can be repaired.
	Safety	How safe it is to operate the device. If the device causes any interference for other devices. Radiation levels. If	How safe it is to operate the device, including electrical safety.	Devices should be safe for patients and meet radiations guidelines.

Theme	*Sub-code*	*H1*	*H2*	*H3*
		the device meets all its certifications.		
	Supplier satisfaction	How satisfied the different stakeholders were with the manufacturer in the past.	There is a formal process in place to evaluate the supplier relation and satisfaction. This evaluation can be used during the procurement process to steer the decision.	Supplier satisfaction is taken into account when a new procurement process is stated. This includes satisfaction with the device itself and the aftersales. When suppliers do not deliver adequate services, they might not be considered in future procurement processes.
Outside influences	*Manufacturers*	Manufacturers will proactively contact doctors to try to sell their new devices. During large procurement processes, they might even continuously seek contact with doctors for an update on the process and ask what they should do to win.	Manufacturers evaluate their relationship with the hospital on a regular interval. Additionally, devices may be installed on a trial basis prior to the final decision. Finally, during the offer evaluation process, manufacturers might be contacted for additional information.	Even though the procurement department is outsourced, there is still direct contact with manufacturers. For example, if doctors have questions about a certain device. The hospital might also have a long-term agreement with a manufacturer where they buy certain devices from the manufacturer over an extended period of time.
	Medical conference	Medical conferences are a way for medical professionals to meet each other, but also for manufacturers to sell their devices. During these conferences, manufacturers will demonstrate their new devices to doctors and try to schedule a follow-up appointment.	Not mentioned.	Not mentioned.
	Other doctors	Doctors from different hospitals will boast about their new shiny devices to each other. Additionally, they will share experiences with certain devices with each other.	Sometimes other hospitals are visited to request their experience with a certain device.	Not mentioned.
Regulations	*Convenant medische technologie*	Not mentioned.	The 'convenant medische technologie' is followed during the procurement process.	The 'convenant medische technologie' is followed during the procurement process.
	GDPR	Not mentioned.	The GDPR is followed.	When data and software is considered, the GDPR also needs to be taken into account.

Theme	*Sub-code*	*H1*	*H2*	*H3*
	MDR	Devices must follow the MDR and are checked whether they comply.	Devices must follow the MDR and are checked whether they comply.	With high-risk devices, a check prior to the instalment of the device is done.
	Medical specialists association	The medical specialists association can publish new guidelines for medical treatments, which hospitals need to follow.	Not mentioned.	The medical specialists association can publish new guidelines for medical treatments, which hospitals need to follow.
	NEN7510	The hospital is NEN7510 certified.	The hospital is NEN7510 certified.	Not mentioned.
	Not tender compliant	Non-academic hospitals are not tender compliant.	Not mentioned.	Not mentioned.
	NZa	The NZa can publish new guidelines for medical treatments, which hospitals need to follow.	Not mentioned.	The NZa can force a hospital to replace a certain device when the regulatory body forbids the use of their current device.
Other	*No acquisition after procurement process*	A procurement process not always leads to a new acquisition. Sometimes during the process, the hospital finds out that the market or technology does not provide yet what they are looking for.	Not mentioned.	Not mentioned.
	Not cybersecure	Sometimes the cybersecurity of medical devices or systems is questioned, based on the ease of sharing data with others.	Since roughly 5 years there is a growing awareness of the importance of cybersecurity, prior that the awareness was low.	Not mentioned.
	Shift to connected medical devices	A shift to connected medical devices is noticeable. Currently, roughly 50% is and 50% isn't connected, whilst it is expected that in the coming years roughly 90 to 95% will be connected.	A shift to connected medical devices is noticeable. This has resulted in a merger between the MedTech and IT department and their processes as they had to work more and more together.	Not mentioned.