Workshop Insights: Navigating Cybersecurity Regulations for Device Manufacturers and Healthcare Operators

Andrea Skytterholm, Lars Halvdan Flå, and Martin Gilje Jaatun

Abstract Both the manufacture and use of medical devices are heavily regulated, but stakeholders have a varying level of maturity, and often struggle to comply with rules and regulations. This paper reports on an empirical elicitation activity that sought to enumerate the challenges faced by (particularly smaller) device manufacturers and device operators (typically hospitals), with a goal to informing the creation of tools that these stakeholders can use to address the challenges. The stakeholders completed a brief survey, and then participated in two focus group sessions delving into perceived challenges. The results confirm a need for increased collaboration between manufacturers and operators, and improved guidance material to ease complying with relevant regulations.

Key words: Cyber security, Connected medical devices, Patient safety, Information security, Privacy.

1 Introduction

The healthcare system faces significant challenges in the coming years, with an increasing number of elderly and ill people and the difficulty of recruiting healthcare workers [18]. Connected medical devices play a crucial role in addressing these challenges. These devices enable continuous monitoring of patient health, allowing patients who previously needed hospitalisation to

Andrea Skytterholm
SINTEF Digital, Trondheim, Norway, e-mail: andrea.skytterholm@sintef.no

Lars Halvdan Flå
SINTEF Digital, Trondheim, Norway, e-mail: lars.flaa@sintef.no

Martin Gilje Jaatun
SINTEF Digital, Trondheim, Norway, e-mail: martin.g.jaatun@sintef.no

receive treatment at home. This shift towards more home-based treatment and care not only enhances patients' quality of life but also presents economic benefits by reducing the burden on the healthcare system and lowering overall healthcare costs.

However, the integration of connected medical devices into healthcare systems introduces a new set of challenges, particularly concerning cybersecurity. As these devices collect and transmit sensitive medical data, ensuring their security is paramount to protecting patient privacy and preventing potential cyber threats. Medical device manufacturers and healthcare operators face specific challenges in identifying and complying with cybersecurity regulations, standards, and guidelines, in the middle of the rapid evolution of technology and the complex regulatory landscape.

This paper aims to investigate these challenges and potential solutions for mitigating them. To guide our work, we have developed the following research questions:

RQ1: What specific challenges do device manufacturers and healthcare operators encounter in identifying and complying with cyber security regulations, standards, and guidelines?

RQ2: What strategies or solutions can be implemented to effectively mitigate these challenges?

By addressing these research questions, the goal is to contribute to increased cybersecurity for connected medical devices, ultimately enhancing the safety, reliability, and effect of healthcare delivery in an increasingly digitalized world.

This paper is structured as follows, Section 2 provides the background of our work. Section 3 describes the methodology used, and in Section 4 we present our findings. Finally, in Section 5 we discuss the results, and Section 6 concludes the paper.

2 Background

The World Health Organization (WHO) has produced a report on the healthcare workforce in Europe and the challenges we are facing in the years to come [18].

In 2019 Levine et al. [8] performed a comparison study of home treatment versus hospital care for patients requiring admission. The results of this study show that administering home treatment for acutely ill adults gives significant benefits compared to hospital care. Home treatment reduces costs and healthcare utilization, besides, it also lowers the rates of readmission. Additionally, patients receiving home treatment demonstrate higher levels of physical activity in comparison with those receiving care in a hospital environment. These

findings underscore the effectiveness and advantages of implementing home-based treatment approaches for acutely ill adults, emphasizing the potential for improved outcomes and reduced burdens on the healthcare systems.

The Code of Conduct for information security and data protection in the healthcare and care services (In Norwegian: "Normen") [17] is created and maintained by organisations and companies in the health sector in Norway, and is used by many of the Norwegian connected medical device (CMD) operators. Normen provides requirements which detail and supplement current regulations, however, it does not cover all the regulatory requirements. The goal of Normen is to contribute to safe and secure information exchange between the different actors in the healthcare sector.

In the US, the Food and Drug Administration (FDA) [3] is responsible for protecting the public health. This responsibility includes ensuring the safety, efficacy and security of medical devices.

3 Methodology

To answer the research questions, we conducted a workshop with 17 participants from the healthcare sector. The participants were recruited from a list of local players in the health technology ecosystem, specifically targeting individuals with competence in regulations, standards, and guidelines for cybersecurity related to CMDs.

Workshop
The participants represented two distinct roles within the healthcare sector, CMD Operators and CMD Manufacturers. Table 1 describes the two roles and provides an overview of the number of participants in each group accordingly.

Workshop agenda:

- Welcome and lunch
- Menti survey
- Breakout session one
- Break
- Breakout session two

The workshop started with a welcoming session and lunch to allow the participants to warm up before beginning the discussions in the breakout sessions. At the end of the lunch, they were given a survey presented in Menti [10]. Menti is a tool designed for creating interactive presentations, quizzes, or surveys. It enables participants to provide real-time feedback or responses. Once the survey is finished, Menti offers the functionality to download the results in a PDF format. The survey was completed in plenary by the participants using smartphones and invited the participants to give input

Table 1 Participants

Role	Description	Number of participants
CMD Operator	Healthcare service providers such as hospitals and healthcare institutions	11
CMD Manufacturer	Manufacturers of CMDs, including developers of software applications	6

on what standards and guidelines they used, and on challenges they faced. In addition to collecting data, the survey also served to start the process of reflecting on these topics. The questions from the survey are presented in Table 2.

Following the survey, participants were divided into three distinct focus groups for the initial breakout session. These groups were formed according to their roles. One group was composed of CMD Manufacturers, while the other two groups were made up of CMD Operators. In the second breakout session, the groups were restructured. The new groups were formed to ensure an even distribution of CMD Manufacturers and CMD Operators. We also strived to distribute participants from the same organization across different groups as much as possible. The workshop was structured in this manner to facilitate discussions on challenges and solutions among participants in similar situations as well as those from different parts of the health ecosystem.

The two focus group sessions each lasted 75 minutes. In both sessions, all groups were presented with 3 to 4 questions to discuss. The questions are presented in Table 3. Participants were instructed to silently write down their responses to each question on a post-it note. Following this, all the responses were collectively reviewed before moving on to the next question. Each group had a facilitator responsible for guiding the discussions, taking notes and keeping track of time.

Data analysis

The data set used for analysis in this work consists of the responses to the survey, the facilitators' notes and the notes from the post-its. After the workshop, the notes taken by the facilitators during the two breakout sessions were processed and completed, and the notes from the post-its were added. The results from the survey were downloaded to a PDF file.

Based on the topics touched upon during the workshop, five main categories, or 'codes', were identified to help analyze the collected data. Some of these main codes also had smaller related codes, or 'sub-codes', under them. All codes and sub-codes are listed in Table 4. After the codes were decided, the data was reviewed and parts were marked based on which code they fit into. This process is known as 'coding'. Once the coding was completed, the coded data was examined more closely to understand what it was indicating.

Table 2 Questions from the workshop survey presented in Menti

Questions:	**Options:**
Which actor do you represent?	Device manufacturer, Integrator, Healthcare provider, Others
Which of the following do you use/fulfil?	GDPR, Medical Device Regulation, In Vitro MDR, Cybersecurity Act, NIS2, Cybersecurity Enhancement Act, Consolidated Appropriations Act, MDCG - Guidance on Cybersecurity for Medical Devices, IMDRF - Principles and Practices for Medical Device Cybersecurity, ENISA - Procurement Guidelines for Cybersecurity in Hospitals, ANSM - Cybersecurity of Medical Devices Integrating Software During Their Lifecycle, eHealth Suisse - Guide for App Developers, Manufacturers and Distributors, BSI - Cyber Security Requirements for Network Connected Medical Devices, Health Canada - Pre-market Requirements for Medical Device Cybersecurity, FDA - Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions, FDA - Postmarket Management of Cybersecurity in Medical Devices, TGA - Medical Device Cyber Security Guidance for Industry, TGA - Medical Device Cyber Security Information for Users, Others
To what extent do standards and regulations ..	Facilitate awareness of cyber security among owners/users of medical equipment, establish a common understanding of legislation and requirements among all parties involved, ensure that the cost of security is in line with the benefit, have purpose and goals that correspond to their needs, are flexible enough to take account of new technology and changes in the threat landscape and risk
Have you experienced contradictions/conflicts in legislation and guidelines between cyber security, ethics and treatment? If so, which ones?	
What challenges have you encountered when using/fulfilling regulations, standards and guidelines regarding ..	Asset management, differences across countries and markets, risk assessments, intrusion detection and logging, incident management and training, complex procedures for certification, different processes in different countries, conduct state-of-the-art analysis, outdated documents and regulations, privacy regulations, lacing standards for OT equipment, regulations lacing focus on security, regulations lacing focus on privacy, how cybersecurity is considered in classification, lack of assessment of the cybersecurity of equipment, lack of protection mechanisms for cybersecurity, others
What are the biggest challenges you experience? when do they occur, why do they occur, and how can they be resolved? Give one or two examples.	

The findings from this examination are written down and can be found in the results section.

Table 3 Questions from breakout sessions

Questions from section 1
1. What standards, guidelines and regulations do you use, and what are they missing? 2. How do you work with cybersecurity? 3. What challenges do you face when following regulations, standards, and guidelines? 4. How do you handle these challenges? What is needed for them to be solved?
Questions from section 2
1. What tensions/conflicts do you observe between cybersecurity, ethics, and clinical care when using standards, regulations and guidelines? 2. How do you handle these conflicts? What is needed for them to be solved? 3. Which area should be focused on in standards, regulations, and guidelines in order to support/realize future scenarios in healthcare?

Table 4 Codes and subcodes used for analysis

Codes	**Sub-codes**
Regulations	MDR FDA Privacy and GDPR
Guidelines	MDCG Normen Filing and certification
Cybersecurity	NIS2 Cybersecurity vs. patient safety
Operators	-
Manufacturers	-
Supply chain	-

4 Results

In this section we present the results from the workshop, structured according to the codes shown in Table 4.

An overview of which regulations and guidelines the participants fulfil/use is shown in Figure 1, as reported by the participants in Menti. For readability, we have excluded the regulations/guidelines which none of the participants

reported as relevant. The full overview of the regulations and guidelines included in the Menti questionnaire can be found in Table 2.

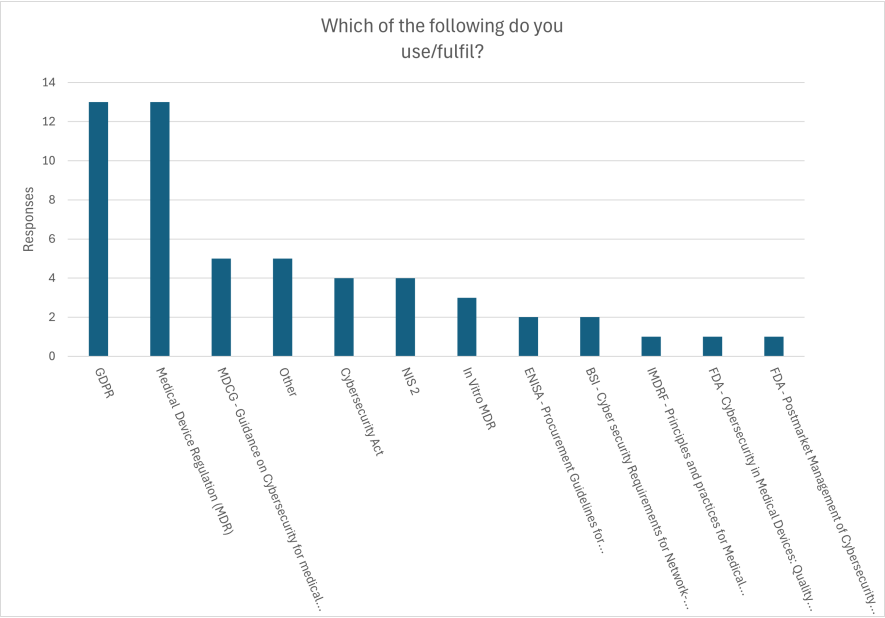

Fig. 1 Standards, regulations and guidelines workshop participants follow

As this workshop was carried out in the context of the Horizon Europe project NEMECYS, a project which also plans to organize similar workshops in other European countries, the questionnaire in Menti focused on international regulations and guidelines. However, during the focus groups, Normen [17], The Act on Medical Devices [13], and NO-18 [15] were also discussed. These are all specific to Norway. The Act on Medical Devices serves as the legal foundation for national regulations and for the execution of directives from the European Commission [13]. NO-18 is a requirements specification document and should be used for the evaluation of the Supplier's offered solution within the areas of ICT and information security [15].

4.1 Regulations

Workshop participants describe the healthcare sector as an extremely regulated sector. Regulatory requirements are one of the major barriers to entry into the market for CMD manufacturers. Workshop participants reported that there is an extensive set of regulations, from many different parties.

They report that it is difficult to navigate the landscape and difficult to get an overview of what they need to consider. Consequently, many new companies struggle to enter the market, and they rarely manage to do so. Not only is it difficult to get an overview, but the lack of resources makes it difficult to keep up with the changes that are made to the regulations and who are affected by such changes. However, although there is an extensive set of regulations, it was reported that there is not much legislation on cyber security. The question raised was if this will become better with NIS2 [6].

"*How can we know which regulations apply to our product? Very segregated laws and requirements, especially when thinking beyond national borders.*" -Workshop participant

Developments of medical equipment are happening faster than the regulations can keep up with. Hence, CMD operators have to say no to new equipment because the regulations do not allow it yet. An example of this challenge is regulations for precision medication and medical genetics algorithms. Machine learning models cannot be changed after they have been approved, because then they are no longer approved.

Another challenge raised by the participants is the challenge of assessing *must* against *should*. There may be different interpretations in situations where the regulations are a bit unclear, and in such situations, decisions from court proceedings become leading. However, it was also said that nobody follows the rules completely, and with medical equipment, you always break some rule or another.

"*Health legislation, privacy legislation, and cybersecurity requirements require a balanced approach, which requires expertise, and often needs to be assessed on a case-by-case basis.*" -Workshop participant

4.1.1 MDR

The starting point of the the Medical Device Regulation (MDR) [5] is "to not harm the patient". However, the MDR is highly relevant to CMD manufacturers but has limited content relevant to the users of CMDs.

One of the challenges concerning the MDR is that they require medical equipment to be developed with regard to the state-of-the-art. Several of the CMD manufacturers participating in the workshop said that it is difficult to understand what is meant by the state-of-the-art, and also what the bar is for something being good enough.

[Challenge:] "*Identify state-of-the-art in cybersecurity for a specific medical device.*" -Workshop participant

Workshop participants stated that some security often leads to reduced usability, which conflicts with the MDR that has a high focus on usability and clinical benefit. The participants used a triangle of security, economy and usability to illustrate this example, and said that you can only get two things. The triangle is illustrated in Figure 2. The participants found it challenging to know where the bar is for when one has to prioritize, and security can be viewed as a barrier or cost.

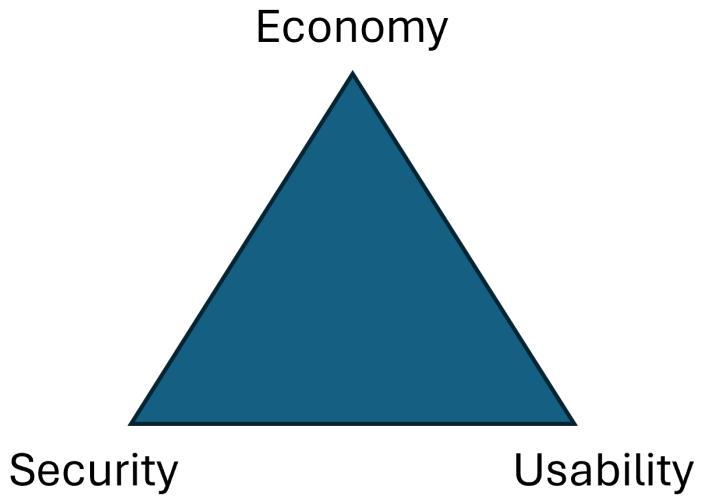

Fig. 2 The security, economy and usability triangle

Regulations apply differently for welfare technology and medical technology. Another finding from the workshop was that it can be challenging for product owners to identify whether their product falls under the MDR regulation or not.

4.1.2 FDA

The FDA [3] guidelines were described as more concrete. However, it was uncertain how they could use standards in and towards the FDA process.

4.1.3 Privacy and GDPR

Workshop participants described privacy as very strict, which could be both positive and negative. Further, they said that compliance with GDPR [4] trumps everything and that it is not always easy to follow the regulations.

However, it was mentioned that it is not always necessary to take the worst path and that there are differences in how pragmatic different regions are. Decisions in court proceedings are leading when the regulations are unclear. Yet, other participants mentioned that privacy legislation is always trumped by health legislation and that there is always a trade-off between privacy and confidentiality, and ease of use.

Another comment made during the workshop was that "GDPR is not a big deal until the Data Protection Authorities come to visit, but this is also the reason why it needs to be kept up to date".

Secondary use of data is another challenge that was mentioned by several of the workshop participants, and especially by the CMD operators. Using data for research and to develop better treatment for patients is of course important, but more importantly, they need to have control over what the data is used for. Another challenge related to this topic is that CMD operators have the impression that many of the suppliers do not have a good enough understanding of what anonymization of data entails. In some situations, suppliers might want to use data to develop better products which can offer patients better treatment, but it is however important that the CMD operators know what they say yes to. An example from Norway shows that it is not always easy to get an overview of the data collected by the supplier and what it is used for. The Norwegian Ministry of Health procured continuous glucose monitors (CGMs) from an American vendor, without being aware that the associated application collected data about the users which was sent back to the vendor and used for various and unclear purposes. It was mentioned that it is important to address who is the owner of the data.

It is not only suppliers who struggle to understand the concept of anonymization, also researchers have made the mistake of using personal data beyond the original purposes. The local hospital participating in the workshop is a university hospital, and many of the employees have positions at both the hospital and the university. In research projects, data have been collected from patient journals and used for purposes other than first intended.

Access control is another challenge. It was mentioned during the workshop that there is an inherent conflict in the GDPR, and one of the workshop participants feared that this might result in people not having the access they should. Access control was also said to be challenging for small companies.

As with the MDR, the GDPR also has requirements for state-of-the-art. However, it is unnecessary to fill out a comprehensive state-of-the-art documentation.

4.2 Guidelines

4.2.1 MDCG

The workshop participants opined that the MDCG 2019-16 guidance [9] is good, but that it should be updated.

4.2.2 Normen

Every operator using services from Norsk Helsenett (a governmental entity providing digital services and infrastructure to the health sector) is required to follow Normen [17]. Many of the operator representatives participating in the workshop follow Normen. Normen provides a set of requirements for suppliers, and one of the main challenges here is that foreign suppliers have no relation to this norm, and also it lacks an English translation of the full text. The technical specification requirements can also be challenging to understand, and some suppliers report that they do not understand them and that they do not know what the operators need from them.

Before Normen, operators had a fact sheet that was formed as a questionnaire, and workshop participants claimed that this was easier to understand. Now, Normen comes with an Excel sheet that replaces the old fact sheet, however, this is not as easy to understand. It is unclear what advice in the sheet applies to them, and it does not use the questionnaire format as in the former document.

It was said during the workshop that nobody fulfils Normen, but that they use a risk-based approach [11]. A risk-based approach is commonly mandated by Norwegian regulatory authorities, and means that the scope of implemented measures according to a given regulation increases where the risk is higher than usual. Conversely, in situations where the risk is lower than usual, the scope of measures can be reduced [11]. This basically the opposite of a rule-based approach. There is a need to balance and consider what is the weightiest consideration. Normen fosters more dialogue between CMD operators and CMD manufacturers.

4.3 Filing and certification

Participants in all groups mentioned that there is an extensive set of regulations from many different parties. Notified bodies are not allowed to advise or consult, but they are the ones responsible for approval. It is difficult to get an answer from the authorities, they prefer not to deal with practical issues or problems.

There might also be a need for a road map to certification. The best thing the EU could have done would be to publish previous filings. We don't know if different notifying bodies have the same practice, and consider the same things when approving a product.

"*Often there is a lack of practical examples of how the requirements can be met.*" -Workshop participant

Very few provide advice on how to do certification. There are major barriers in place for new actors, where is the bar for certification? Not a single example exists of what an approved filing/process looks like. The process is also complicated by the fact that sometimes one only has to comply with parts of a standard.

4.4 Cybersecurity

4.4.1 NIS2

One challenge mentioned is that cybersecurity costs money, but there is no return of investment here. NIS2 [6] makes it possible to fine cybersecurity violations, which can result in cybersecurity no longer being seen only as an expense. No one would like to buy equipment which can cause your organisation fines in the order of millions.

4.4.2 Cybersecurity vs. patient safety

Balancing cybersecurity and patient safety is a real challenge, and there are several reasons for that. Clinicians and patients most often care about clinical benefit, and their primary focus is not on regulations and security. In clinical settings, the primary focus is on patient care and security requirements will be viewed as something cumbersome and can be experienced as a barrier for the clinicians. One participant claimed that it is ethically problematic to stop good projects due to legal requirements. Cybersecurity practices may conflict with patient safety as cybersecurity can affect usability and make it difficult to use the device. One example of this is two-factor authentication. One of the workshop participants mentioned that they had implemented two-factor authentication for their app, however, as their patients are people struggling with anxiety and depression, two-factor authentication increased the threshold for using the app. This example also shows how important it is to follow technological development, and the solution to this problem was solved by replacing BankID (a personal identification method [1]) with biometry, the threshold was thereby lowered.

[Identified conflicts between cybersecurity, ethics and patient treatment:] "*There is a challenge in terms of usability*" -Workshop participant

During the initial discussion, cybersecurity and patient safety were viewed as two different things, however, it was also mentioned that cybersecurity aligns with patient safety. One of the CMD manufacturer participants stated that they regard cybersecurity as part of patient safety but that some hospital people regard cybersecurity as something separate.

"*In tenders, ICT security is often deprioritized by clinicians. But information security also provides patient safety. This needs to be made more aware*" -Workshop participant

A third view on this is the balance of risk and benefit. When developing a product, you need to consider the clinical benefit, and the effect of the product should weigh more than the harm it causes. A risk management plan can be used to report cybersecurity risks, which in turn can translate to patient risk. Cybersecurity can again lead to new risks to patient safety, so this balance is a challenge. It was said that it is usually easier to be better safe than sorry, which in turn affects user-friendliness in some situations.

Another challenge the CMD manufacturers raised was that you do not know who will manage the device. Is it a doctor at the hospital, a home nurse or the patient himself? Depending on who operates the equipment, different challenges will arise. The technological maturity of the user is also something that needs to be considered in this situation.

4.5 Operators

The focus of the CMD operators is on operation and maintenance, and here The Act on Medical Devices [13], MDR [5] and GDPR [4] have a central role. CMD operators focus on making the manufacturers responsible for compliance with regulations and standards.

In a procurement process, CMD operators communicate with the sellers of the product, these are not necessarily the ones with the technical specification knowledge. This extra link in the communication process is perceived as a barrier to obtaining the necessary information.

The total purchases made by CMD operators in Norway are small compared to the purchases made by large hospitals in the U.S., thus, CMD operators find it challenging to put requirements on CMD manufacturers, when they respond that the device is FDA-approved.

Another challenge mentioned is that new systems brought in are not new but legacy systems that do not follow the relevant standards and guidance, nor do they comply with current regulations. However, they must be used because there are no available alternatives on the market. It takes time to

get the certifications in place. The solution in such scenarios is to have them operate in a closed network that does not communicate with the hospital network. This allows operators to use it as a standalone solution.

"*Cybersecurity should not be seen as an expense, but as an investment*" -Workshop participant

CMD operators claimed during the workshop that they are good at complying with regulations, however, not enough resources have been allocated to deal with this. As a result, it is easier to say no to new CMDs rather than familiarizing themselves with the regulation and taking the time to keep up with the developments. From a political point of view, the healthcare sector will be digitalized, however, CMD operators find this challenging when they do not have enough resources to build competence within the organisation.

4.6 Manufacturers

CMD manufacturers reported that they find it challenging when the requirements put forward by the hospitals are different from those in standards and regulations. CMD manufacturers need more information about what is required to market and sell products, and it is important to get this information early in the development process to prevent them from ending up on the wrong track.

The findings from the workshop show that it is unclear whether it is the manufacturer or the operator who has the responsibility for the update of the CMDs. Some workshop participants claim that the manufacturer is not required to perform the update, whereas others claim that CMD operators demand over-the-air updates and require equipment to be kept updated by the manufacturer.

4.7 Supply chain

When CMDs are certified, they are certified by themselves, but one of the challenges mentioned is that this certification does not consider the situation when the CMD is integrated with the hospital systems. One question raised regarding this topic was about the demarcations for responsibility in this scenario. Every integration into a hospital is different, and a risk assessment is needed in each case.

One of the concerns raised by some of the workshop participants was related to the integration of CMDs and the division of responsibility. What is the CMD operator's responsibility and what is the CMD manufacturer's responsibility? In the requirements specification NO-18 there is a self-declaration

that covers parts of this responsibility challenge, but NO-18 has more focus on the operational side [15]. It is unclear who is responsible for the configuration of a product so that it is integrated securely, and it is unclear how this is done in practice. Also, the main point of this is who is left with the risk?

5 Discussion and Conclusion

What specific challenges do device manufacturers and healthcare operators encounter in identifying and complying with cyber security regulations, standards, and guidelines? And what strategies or solutions can be implemented to effectively mitigate these challenges?

The healthcare sector is heavily regulated, which causes significant barriers to entry for CMD manufacturers. Navigating the complex landscape of regulations, standards and guidelines from various authorities is challenging, often resulting in new companies struggling to enter the market. Additionally, the rapid technological development exceeds regulatory updates, leaving CMD operators struggling with outdated regulations that prevent them from accepting innovative medical equipment.

One of the main challenges for CMD manufacturers is to get an overview of all the relevant regulations, standards and guidelines they need to consider when developing new medical devices. It is not only resource-demanding to identify the right documents but also to identify which parts of the documents are relevant.

Normen [17] may also be considered a challenge for the CMD operators. It provides a framework for compliance, but with no English translation, it is difficult to convince foreign suppliers to follow the requirements. Also, Norway is such a small country, and some procurements even happen at the hospital level, meaning that the procurements are quite small compared to the ones in the U.S. Furthermore, the lack of clarity on responsibility and integration issues within the supply chain adds another layer of complexity.

The MDR [5] emphasizes patient safety but lacks clarity on state-of-the-art requirements, creating uncertainty for manufacturers. Balancing security, usability, and economic considerations further complicates compliance efforts, especially concerning cybersecurity and privacy regulations such as GDPR [4].

Access control was identified as a challenge, particularly for small companies. One participant expressed concern that many individuals do not have the necessary access rights, and that access control is one of the primary challenges with Norway's newest journal system. However, the issues with access control are two-fold. On the one hand, some healthcare personnel do not have the access rights they need [12]. On the other hand, healthcare personnel have access to data they should not be able to access [14]. This highlights the complexity and importance of effective access control in healthcare systems,

especially when implementing new journal systems. As mentioned during the workshop, there is an inherent in the GDPR. The inherent conflict can be viewed as the challenge of balancing the need for access and at the same time limiting the level of access to what is strictly necessary.

Cybersecurity emerges as a critical concern, with the introduction of NIS2 [6] potentially shifting perspectives by imposing fines for violations. However, balancing cybersecurity measures with patient safety remains a challenge, highlighting the need for adaptable solutions that prioritize usability and clinical benefit.

To tackle these challenges effectively, stakeholders need to work together. This means simplifying regulatory procedures, clarifying who's responsible for what, and encouraging innovation — all while prioritizing patient safety and data privacy.

Working together is essential for the healthcare sector to make the most of CMDs and improve patient outcomes. These insights emphasize the need for ongoing communication, updating regulations as needed, and investing in the resources and expertise required to overcome regulatory challenges and fully utilize the potential of CMDs in transforming healthcare delivery.

5.1 Threats to Validity

This paper has reported on just a single workshop with a small number of participants from a limited geographical area in a small European country, and thus cannot lay claims to generalizability in a global or even European context. However, Norwegian manufacturers generally market their devices to a European or global audience, and are thus likely to face similar challenges as experienced by other European manufacturers. Furthermore, Norwegian health care providers (or operators) are subject to MDR and GDPR just like their European counterparts. The results from our workshop are also aligned with our previous work [2].

5.2 Further Work

The results reported in this paper will inform the ongoing work of the Horizon Europe NEMECYS project [7], where we are building tools that will help device manufacturers to better comply with MDR through building security in to connected medical devices, as well as tools that will assist operators in better ensuring security in the use of their connected medical devices, and improving the privacy of patients. The empirical work reported in this paper is being complemented by similar workshops conducted in Spain, Italy and Greece, and results from these will appear in subsequent publications. We

have also formed a collaboration with four other Horizon Europe projects working on enhancing cybersecurity of connected medical devices, and this work has already resulted in a initial feedback on how the MDCG 2019-16 guideline can be improved [16].

References

1. BankID: What is BankID?, https://bankid.no/en/what-is-bankid
2. Bernsmed, K., Jaatun, M.G.: Security-by-design challenges for medical device manufacturers. In: EICC 2024. ACM (2024), https://jaatun.no/papers/2024/HealthSec_Barriers.pdf, to appear
3. Center for Devices and Radiological Health: Cybersecurity in medical devices: Quality system considerations and content of premarket submissions (2024), https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions
4. European Commission: 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), https://eur-lex.europa.eu/eli/reg/2016/679/oj
5. European Commission: 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 (2017), http://data.europa.eu/eli/reg/2017/745/oj
6. European Commission: 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), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555
7. Jaatun, M.G., Taylor, S., Upstill, C., Farkash, A., Garcia, S., Andoutsos, C.: Nemecys: Addressing challenges to building security into connected medical devices. Procedia Computer Science (2024), https://jaatun.no/papers/2023/nemecys_longer_paper.pdf, to appear
8. Levine, D.M., Ouchi, K., Blanchfield, B., Saenz, A., Burke, K., Paz, M., Diamond, K., Pu, C.T., Schnipper, J.L.: Hospital-level care at home for acutely ill adults: a randomized controlled trial. Annals of internal medicine **172**(2), 77–85 (2020)
9. Medical Device Coordination Group: MDCG 2019-16 - Guidance on Cybersecurity for medical devices (2020), https://ec.europa.eu/docsroom/documents/41863
10. Mentimeter: Mentimeter. https://www.mentimeter.com/, accessed: 03.05.2024
11. Ministry of Finance: Prop. 40 L (2017–2018) (Feb 2018), https://www.regjeringen.no/no/dokumenter/prop.-40-l-20172018/id2589604/, publisher: regjeringen.no
12. Patterson, R., Standing, H., Lee, M., Dalkin, S., Lhussier, M., Exley, C., Brittain, K.: Paramedic information needs in end-of-life care: a qualitative interview study exploring access to a shared electronic record as a potential solution. BMC Palliative Care **18**, 1–8 (2019)
13. Lov om medisinsk utstyr (*the act on medical devices* (2020), https://lovdata.no/dokument/NL/lov/2020-05-07-37

14. Støbakk, T., Skjesol, H.: Datatilsynet varsler tilsyn med helseplattformen etter flere brudd på personvernet. https://www.adressa.no/nyheter/trondelag/i/O8Gm4l/datatilsynet-varsler-tilsyn-med-helseplattformen-etter-flere-brudd-paa-personvernet, accessed: 08.05.2024
15. Sykehuspartner HF: No-18 - kravspesifikasjon for medisinsk teknisk utstyr (MTU) med tilhørende IKT-grensesnitt v1.5 (*no-18 – requirements specification for medical technical equipment with associated ict interface* (2024), https://www.sykehuspartner.no/490b0f/siteassets/documents/sikkerhet---regionale-bruksvilkar/no-18---kravspesifikasjon-for-mtu-medisinsk-teknisk-utstyr-med-tilhorende-ikt-grensesnitt.pdf
16. Taylor, S., Jaatun, M.G., Bernsmed, K., Androutsos, C., Castillo, A., Frey, D., Favrin, S., Rodrigues, J., Milojevic, D., Karas, D.S., Siachos, I., Gedeon, P., Epiphaniou, G., Moukafih, N., Maple, C., Messinis, S., Rallis, I., Protonotarios, N.E., Matragkas, N., DeLong, R., Arvanitis, T., Katzis, K.: A way forward for the MDCG 2019-16 medical device security guidance. In: Proceedings of PETRA 2024 (2024), https://jaatun.no/papers/2024/PETRA-HLTH-13-Collaboration-Paper-MDCG-final.pdf, to appear
17. The Norwegian Directorate of Health: The code of conduct for information security and data protection in the healthcare and care services (2022), https://www.ehelse.no/normen/documents-in-english
18. WHO Regional Office for Europe: Health and care workforce in Europe: Time to act (2022)