# Patching Up: Stakeholder Experiences of Security Updates for Connected Medical Devices

Lorenz Kustosch
*TU Delft*

Carlos Gañán
*TU Delft*

Michel van Eeten
*TU Delft*

Simon Parkin
*TU Delft*

## Abstract

Medical devices become increasingly connected and thus require security measures to ensure patient safety and data protection. However, such connected medical devices are often reported to lack basic security and to run on unpatched and outdated software. Thus, there is an increasing push to deliver security patches faster and more regularly to devices in the field. In this work, we empirically study current practices of patching connected medical devices by conducting 23 semi-structured interviews with participants from nine healthcare delivery organizations (HDOs) and three medical device manufacturers, also capturing data on actual updating practices for 25 specific medical devices. We find that delivering software updates to medical devices is an laborious and costly process for HDOs and manufacturers, as operational demands for medical use and an increasing need for infrastructure management put significant strain on involved stakeholders, thus rendering it questionable if conventional security patching will actually work in the healthcare sector without overwhelming it operationally and financially.

## 1 Introduction

Healthcare Delivery Organizations (HDOs), such as hospitals, clinics, and practices, operate with an increasing number of medical devices connected to their network. Think of imaging, patient monitoring, or surgery equipment. A key measure to secure any networked device from attacks is to regularly provide software updates to address vulnerabilities. However, it has been repeatedly reported that a plethora of connected medical devices remain outdated and vulnerable. The prevalence and risks of unpatched and outdated medical devices have been raised by governmental actors such as the FBI [46], industry reports [5, 10, 29], and academic studies [24].

The security risks of connected medical equipment have led to a regulatory shift, such as the PATCH Act, which mandates the U.S. Food and Drug Administration (FDA) to require manufacturers to continuously release security patches over the lifetime of medical devices [27]. Similarly, the E.U. Medical Device Regulation (MDR) requires manufacturers to respond to security risks with potential patient safety implications (e.g., with a security patch) and upcoming regulations in Japan require manufacturers to follow the IEC 81001-5-1 standard, which also defines a continuous risk management and patch release process for medical equipment. The regulatory pressure on manufacturers to release timely patches only makes sense if the HDOs deploy them, which would lead to an increased patching frequency of medical devices in the upcoming years.

It remains unclear, however, how faster patching cycles for medical devices interact with the operational status quo in hospitals. Prior studies [14, 24, 32, 34, 48] have interviewed IT and health professionals about the broader challenges of providing cybersecurity in HDOs. In most cases, patching is only mentioned in passing, if at all. That said, this line of research does consistently observe a difficult tension between security requirements and the operational pressures to deliver health services. Dissanayake et al. [14] did study patching in healthcare, but for conventional IT, not medical devices. The closest related work to our study is [24]. The authors interviewed eight IT professionals, also covering challenges of patching medical devices. However, the IT department is usually not actually deploying the patches to medical devices. That is typically done in the medical departments by so-called biomedical engineers. So the study provides an indirect view of IT professionals on the updating of medical devices.

We present the first study on the security updates of medical devices based on interviews ($n = 20$) with biomedical engineers and other professionals who actually control the devices and their patches. These interviews were conducted in 9 HDOs in the Netherlands, Italy and the U.K., typically responsible for thousands of connected medical devices. We complement these observations with interviews with three leading device manufacturers ($n = 3$) since patching actions might be conducted by the manufacturer's field technicians.

The purpose of this study is to understand how the process of updating connected medical devices in their operational environment at HDOs is implemented and managed, and what this process translates to with regard to security, patient safety, and operational effort for the involved stakeholders. We pursue two research questions: *(i)* How are connected medical devices patched within their operational environment at HDOs? and *(ii)* What kind of challenges do HDOs and medical device manufacturers encounter during this process and how are they mitigated? In short, we make the following contributions:

- We provide novel evidence on the patching of medical devices in hospitals and find that around half of the HDOs try to patch devices as much as possible by themselves, while the others mostly outsource it to manufacturers or third-party providers. Rarely were patches deployed remotely, even though this option often exists. No HDO was able to install patches for all devices by themselves.
- No HDOs tracked vulnerabilities and all available software updates for their devices. They wait to be alerted by manufacturers or authorities. The frequency of update deployment varied greatly across device types and organizations, from once every 3-4 years to every 2 months. A rough mean for the examples we discussed was around once per year. In many cases, it was unclear to our respondents if their patching kept up with the release cycle of patches.
- We extend prior work on the security of connected medical devices by highlighting various factors that impact patching, such as cost. In some cases, patches are bundled with software updates that need to be paid for. Two participants mentioned that applying a single update on a single device would cost around 10,000 euros. Even when patches are free, the services of manufacturer field technicians are "expensive".

In the next section, we introduce the background and related work for our study, including the regulatory environment. After that, we turn to the methodology, our results, discussion, and conclusions.

## 2 Background and Related Work

This work focuses on physical connected medical devices specifically used for patient care at HDOs. We define them as cyber-physical systems used for hospital patient care, such as monitoring, diagnosis, surgery, and/ or drug delivery that are equipped with network capabilities. Thus, this study does not focus on medical equipment for patients' homes, more consumer-grade health-related IoT devices (such as wearables), or software-as-a-medical-device (SaaMD).

### 2.1 IT Security in the medical domain

Previous work studying IT security at HDOs frequently mentions the increasing connectivity of medical devices and end-point complexity as a significant risk factor increasing healthcare providers' vulnerability [2, 8, 32]. Security updates are also regarded as important for the cyber-resilience of HDOs [8]. A range of proof-of-concept attacks on connected medical devices have been demonstrated, such as hacking an insulin pump [47] or accessing a hospital's picture archiving and communication system via a connected CT scanner [43]. Medical staff may also have difficulty in detecting manipulated readings of a connected patient-monitoring system [56].

However, empirical work on how such medical IoT devices are actually deployed in their operational environment, how they are secured, and the organizational practices around them, is scarce. Previous work, via HDO scans or Shodan, has identified vulnerable and misconfigured connected medical devices [15, 39, 54]. Prior work has not considered if and how devices are patched, and how affected HDOs manage related risks organizationally.

One of the few empirical accounts [24] reported severe challenges, such as significant delays in patching, a disorganized process that varies across devices, vendors, and hospitals, and staff's uncertainty concerning patch prioritization and timing. Coventry et al. [9] reported on hospital staff not feeling adequately prepared for the security implications of connected medical devices and the general diffusion of responsibility outside of typical biomedical or IT departments.

### 2.2 Patching practices

Although there is prior research of patching behaviours for end-users [16, 25, 38, 53], and systems managers in organizations [3, 11, 33, 36, 49], empirical literature on patching IoT devices within organizations is limited.

Li et. al. [36] studied how system administrators implement and manage the patching process within organizations. Challenges were noted, such as difficulties in determining the availability of patches, bug fixes and security updates competing for prioritization, incremental testing and roll-out of updates, and updates introducing problems of their own. Other studies about patching practices from the system administrator perspective reach similar conclusions. [3, 14, 49].

Building on this work, Dissanayake et. al. studied sociotechnical factors of the patching process within the healthcare sector, in a series of studies with a governmental health services agency and an IT service provider in Australia [12–14]. The participating organizations provided (security) updates to customers' IT server infrastructure, which could also be running hospital applications, such as Electronic Medical Records (EMR). The authors report on struggles with coordinating the patching process across varying departments, customers such as hospitals (e.g., due to the resulting system downtime), and medical software vendors, often resulting in delays. Further challenges include technical dependencies and compatibility issues with existing hard- and software (including outdated OS systems), and the mental overload for system administrators, who have to manage an increasing number of configuration options, patch releases, and software versions in a heterogeneous IT environment.

While previous work provides important insights into the updating practices of conventional IT (such as servers and workstation PCs) from the perspective of IT experts such as system administrators, it does not study connected medical devices nor HDOs' perspective on how this critical infrastructure is managed, secured, and updated.

## 2.3 Regulatory landscape of medical IoT devices

Medical devices are heavily regulated due to patient safety, which also impacts security implementations and the software updating process. Here we consider a selection of key regulations for connected medical devices from major markets. Medical device manufacturers often harmonize their processes to comply with most regulations worldwide. Thus, the Food and Drug Administration's (FDA) rules from the USA usually also apply to medical devices being developed and sold in other markets.

Depending on the medical device class and associated risk level, manufacturers have to provide documentation to the FDA and get premarket approval for devices considered high-risk. The evolving security risk landscape for connected medical devices has led to the introduction of the PATCH Act, which defines new cybersecurity requirements for connected medical devices to be enforced by the FDA [1]. From October 2023 onward, to receive premarket approval, medical device manufacturers have to demonstrate to meet these requirements, which include postmarket surveillance of security vulnerabilities and having processes in place to release security patches on a '*reasonably justified regular cycle*', and for critical vulnerabilities, '*as soon as possible'*. This does not apply to devices already on the market unless any change to the device would require another premarket submission. Previously, the FDA provided non-binding security-related guidelines for manufacturers [26, 28].

In the EU, another influential market for devices, connected medical devices have to comply to the Medical Device Regulation (MDR) [51]. For a medical device to receive the CE label and be sold within the EU, it is assessed for adherence to the MDR's requirements by a notified body. Furthermore, the NIS2 Directive [52] directs member states to ensure that operators of critical infrastructure like HDOs take appropriate security measures, such as adopting cyber hygiene practices like software updates, while the GDPR [50] establishes requirements on data protection.

According to the MDR, medical device manufacturers need to ensure patient safety over the device's lifespan. Thus, security risks that could impact patient safety have to be resolved and changes to the device's hard- or software have to be validated to ensure continued safety. Thus, for any software update along the device's technology stack (e.g., an OS security update), the manufacturer needs to go through a validation process, which impacts the update release time. The operator can only install a software update on a medical device that has been validated by the manufacturer.

In the UK, the Medicines and Healthcare Products Regulatory Agency (MHRA) regulates the market and medical devices need to comply to the UK Medical Devices Regulation 2002 [21]. The National Health Service (NHS) provides cybersecurity guidelines for HDOs (e.g., [45]). Regulations in the UK are currently in transition, with EU CE-marked devices still being accepted in the coming years, yet future regulations are in development [42].

A recent regulatory push comes from Japan, where medical device manufacturers are required from April 2024 onward to continuously improve devices' software security with patches according to IEC 81001-5-1 [31], regardless of an acute critical risk [22]. Thus, regulators increasingly recognize the importance of connected medical device security, and a general trend towards more rules for frequent and timely patch releases is observed.

# 3 Methodology

To explore patching practices of connected medical devices empirically, we conducted semi-structured interviews with 20 stakeholders at HDOs and three product security experts from three different major medical device manufacturers between July 2023 and January 2024. All participants were involved in the patching process of medical devices in some capacity, which allowed us to understand the process more holistically.

During the interviews, we also probed for details on the patching process of actual devices and thereby collected 25 cases of varying updating processes. This allowed us to collect rich data on the actual practice of patching and its inherent variability across medical devices, operational contexts, and organizational structures, painting a picture of a heterogeneous, complex, and, at times, ad-hoc process.

## 3.1 Recruitment and Participants

As we expected general IT and updating practices to differ across HDOs and devices, we collected data from various HDOs to get a broader sample. The majority of the HDOs were recruited in The Netherlands as the researchers' country of residence, yet we also included HDOs from the UK and Italy to capture country variability. Medical device manufacturers were also European, two of which were headquartered in Germany and one in The Netherlands.

We recruited participants who are involved in the patching process of medical devices in some capacity, such that they either (i) are included in the decision-making around software updating processes, (ii) implement and/ or roll out updates, or (iii) are involved with product security at manufacturers.

To recruit a sample from this hard-to-reach population [17], we first leveraged our professional network and research project consortium to reach out to stakeholders working in the healthcare sector as initial points of contact. With these professionals brokering contact, we identified and contacted relevant organizations, explained our research plans, and asked relevant stakeholders to participate in an interview. In total, nine HDOs and three medical device manufacturers agreed to participate. During the interviews, we applied snowball sampling [20] by asking interviewees for references to colleagues in similar positions at the same or other organizations.

Notably, the roles and departments involved in software updating of medical devices varied across hospitals. Thus, participants with varying roles at HDOs and medical device manufacturers took part in our study. Participant demographics are depicted in Table 2.

## 3.2 Study Design

To determine the research design, we began with an exploratory phase, in which we conducted pilot interviews based on our research questions and a review of previous literature. We interviewed six practitioners involved in security of connected medical devices, four of which were involved in the patching of medical devices at a hospital and two at a medical device manufacturer involved in product security with customer contact. During the interviews, we gained an initial understanding of the process of software updates for medical devices, stakeholders' responsibilities, and any challenges they faced. Based on these results, we designed the protocol for the final semi-structured interviews. Results from the pilot interviews were not included in the final analysis.

We designed a different interview protocol for HDOs and medical device manufacturers, as roles and responsibilities regarding security updates of medical devices differ between the two actors. However, as the focus of this work was to understand patching practices of medical devices at hospitals, we aimed at recruiting as many participants from HDOs as possible, while the manufacturer interviews provided additional context on the patching practices reported at HDOs.

After the first four interviews, we slightly adjusted some questions' wording and sequence but retained the overall structure and content. Slight adjustments of interview questions during data collection are accepted and even recommended for such action research by methodological literature (e.g., [40]), as it allows the researcher to respond to emerging, unexpected themes to probe for them more thoroughly in subsequent interviews.

## 3.3 Interview Procedure

Opening the HDO interview after collecting informed consent (see Section 3.5), we began with general questions about the participant's role, followed by how connected medical devices and their security are managed within the HDO. We then asked interviewees to walk us through the process of how these devices receive security updates. At this point, we asked about details of the last three times they installed a security update on a medical device. Specifically, we were interested in the device type, how they learned about the patch, the timing of patch release and installation, the installation process, and how the device was actually connected to the rest of the HDO (e.g., to which networks and other devices).

This way, we captured a sample of 25 software update instances across eight different HDOs from 14 different manufacturers to ground stakeholder perspectives in practice. Twelve interviewees provided such update instances, but not all were dedicated security updates; there were also bundled software updates that might include security aspects, making it impossible for participants to entangle them. Participants not providing these update cases were either not directly involved in *installing* the update but more involved with the managerial decision-making or network surveillance or were not aware of any software updates on their fleet of medical devices. The column "*# cases*" in Table 2 denotes how many software update instances the participant contributed.

Interviews with participants from manufacturers followed a similar structure, beginning with the interviewee's role, followed by how frequently their products in the field receive (security) updates, how risk is assessed and decisions concerning security patches are made, how exactly updates reach devices in the field, and how they retain an overview of their products at HDOs. The full interview protocols for HDOs and medical device manufacturers can be found online[1].

In total, three interviews (P2-H1, P5-H1, and P15-H6 & P16-H6) were done in-person and 14 remotely via video conference tools. Most interviews were done between one participant and the researcher, while during four interviews, there were between two (P3-H2 & P4-H2, P15-H6 & P16-H6, and P19-H9 & P20-H9) and three (P7-H3, P8-H3, & P9-H3) participants present due to participants' tight schedules or the necessity to involve colleagues from varying backgrounds. All interviews were conducted by the primary researcher in English, while one interview (P15-H6 & P16-H6) was conducted in Dutch with the support of a second dutch speaking researcher. Two participants (P1-H1 & P12-H5) could not participate in person or did not want to be recorded, so we asked the interview questions via email. Interviews took 51 minutes on average (Range: 28 - 65 min).

## 3.4 Data Analysis

We analyzed interviews using thematic analysis and continued data collection until reaching theoretical saturation in the HDO interviews when no new meaningful theoretical themes emerged from the data [23, 40]. Interviews were recorded

[1] https://doi.org/10.4121/71a01e8f-b432-4a40-b922-c1e1a07b86f7

and then transcribed. The transcripts were analyzed by the primary researcher via open coding, annotating any emerging themes and creating an initial codebook (with one coder regarded as being appropriate for this form of coding [4]). After the first five interviews, the code book was discussed with three other researchers with varying backgrounds and codes were adjusted to better fit the data. This process of validation and refinement of the code book was continued until theoretical saturation was reached. The final refined codebook was then applied to the previous interview transcripts to ensure standardized coding across all interviews. Notably, we did not reach full saturation with the manufacturer interviews due to the small sample ($n = 3$). We do also report these findings, as our goal was to (i) complement and provide commentary from a different perspective on our observations at HDOs and (ii) present novel insights for the academic community, as security research involving medical device manufacturers is very scarce. The final codebooks are provided online[1].

## 3.5 Ethics and Data Protection

The study was approved by the researchers' institution's human research ethics committee. Before the interview, participants were informed via informed consent and orally by the primary researcher about the study's purpose, that participation was voluntary and not compensated, and the data collection process; Transcripts and quotes were anonymized and transcripts, audio recordings, and all interview responses were exclusively stored on a secured network at the researchers' institution. The paper draft was shared with participants before publication for review and potential retraction of any quotes or results. No participants requested any changes to quotes or results due to privacy and/or ethical concerns.

Four interviews were conducted with more than one participant present and thus at risk of negatively affecting participants' safety to speak up in front of colleagues. However, this multi-person interview format was actively suggested to us by the respective participants due to the distributed knowledge or time constraints. Thus, participants arranged and agreed internally to do the interview together as a group without the researchers requesting this. In each multi-person interview, every participant raised their voice, as they were experts on their respective topics.

# 4 Results

To understand the process of patching connected medical devices at HDOs, we first examine the infrastructure the devices are embedded in, describe security update delivery pathways, and contextualize these findings with manufacturers' perspectives. When referring to specific participants, we use the denotation "*P_-H/M_*", where *P_* precedes the participant's ID and *H_* or *M_* the HDO or manufacturer ID, respectively.

| HDO ID | Country | # Employees | # medical equipment | # connected med. equip. |
|---|---|---|---|---|
| 1 | NL | 4,000 - 4,999 | 10,000 - 14,999 | NA |
| 2 | NL | 3,000 - 3,999 | 10,000 - 14,999 | 500 - 999 |
| 3 | ITA | 2,000 - 2,999 | 5,000 - 9,999 | < 500 |
| 4 | NL | 3,000 - 3,999 | 10,000 - 14,999 | 3,000 - 3,999 |
| 5 | NL | 6,000 - 6,999 | NA | < 500 |
| 6 | NL | 4,000 - 4,999 | 10,000 - 14,999 | 3,000 - 3,999 |
| 7 | NL | 4,000 - 4,999 | 15,000 - 19,999 | 3,000 - 3,999 |
| 8 | UK | 20,000 - 24,999 | 75,000 - 100,000 | 4,000 - 4,999 |
| 9 | UK | 25,000 - 29,999 | 75,000 - 100,000 | 3,000 - 3,999 |
| Manu. ID | Country | # Employees | | |
| 1 | DE | 60,000 - 69,999 | | |
| 2 | NL | 60,000 - 69,999 | | |
| 3 | DE | 10,000 - 19,999 | | |

Table 1: Overview of participating organizations' country of headquarters, size, and medical equipment inventory of HDOs. The numbers of medical equipment and connected medical equipment were estimations by participants

## 4.1 Infrastructure

Due to substantial observed variance across HDOs in managing connected medical devices and their security updates, we start by describing HDO infrastructures, processes, and responsibilities to understand what is actually being patched.

### 4.1.1 Device estate of participating organizations

Table 1 depicts HDOs' sizes and reported inventory of medical equipment. HDOs participating in this research varied in size, ranging from below 3.000 employees to more than 25.000. This size was also represented in the number of medical equipment in use. We had no insight into exact asset management systems, but the numbers reported to us give a general indication of the magnitude of inventory size. At the HDOs in our sample, this was easily in the thousands, ranging from around 5.000 to more than 75.000 individual medical devices of varying sizes and uses.

When asked for the number of connected medical devices among the total number of medical devices, numbers diverged. For some participants, this was not actively tracked, or they were only able to answer for their own departments. Others, however, had a more precise overview, as connected devices were registered in their systems in some way (e.g., via asset management tools or MAC addresses in the network access control system). As a coarse estimation, the number of connected medical devices at the HDOs ranged from hundreds (e.g. H3), to thousands (e.g., H8). Participants generally expected these numbers to rise, as "*(...) it is very hard these days to buy equipment that measures something that is not connected to a network or a server.*" (P13-H6).

### 4.1.2 Management and discovery of devices

All HDOs had an asset management system in place to track the inventory of connected medical devices. The majority used Enterprise Asset Management (EAM) software, in which medical devices, spare parts, and maintenance tickets were tracked. Yet, localizing the physical devices could be non-trivial, even when listed in an inventory database. Participants from four HDOs (ID 4, 6, 8, & 9) mentioned that, especially for devices in high numbers, like infusion pumps or bedside monitoring equipment, it would take long, or almost be impossible, for technicians to locate all devices when installing updates, as they had no insight into the devices' (alternating) location, even when devices were visible on their network traffic. Two participants explained how they would love to put Air Tags on each device after the next update to be able to find them again.

No HDO reported actively tracking software versions, available updates, and vulnerabilities of all their connected medical devices, as they would for conventional IT systems. However, four HDOs (ID 4, 6, 8, & 9) reported tracking software versions of medical devices via their EAM software, which required manual input after each update. While participants generally voiced content with this system, they acknowledged that "*it's hard but people manage.*" (P11-H4).

### 4.1.3 Department structures and interactions

Traditionally, medical equipment at HDOs is maintained by medical technology (or "clinical" or "biomedical" engineering) departments. However, due to devices' increasing connectivity, IT expertise becomes essential. This merging of disciplines also became evident in our study. We thus report on the observed departmental structures and distributed stakeholder responsibilities concerning software updates of medical devices, as this is fundamentally different from organizational patch management of more conventional IT infrastructure, which is usually done by system administrators [3, 36, 49].

Several HDOs (ID 1, 3, 4, & 6) combined their IT departments with medical technology departments within the last years. This integration was either done by incorporating medical technology fully into the IT department, including them into an umbrella cluster with its own management, or extending the IT department's responsibilities to medical device security while keeping technical maintenance with the medical engineering department. The two UK HDOs were NHS Trusts and much larger organizations. Thus, they generally had more specialized technical and inventory management departments and cross-department committees and projects were appointed for specific tasks or projects to combine expertise from these different highly specialized branches.

Both IT and medical engineering shared responsibilities for connected medical devices, with the network infrastructure usually being managed by IT, and the physical devices and their interfaces to networks by medical engineering. However, they were commonly referred to as two different worlds with widely different approaches and expectations. This included mismatched processes (IT-based change management and SCRUM sprints clashing with medical engineering practices) or differing expectations for a medical device's lifespan (10 to 15 years seen as normal by medical technicians but long for IT) and patch frequency (IT departments favored regular updates like "Patch Tuesday," while technicians preferred fewer changes to functional systems). P2-H1 remarked; "*...the IT guys, they love updates (...), but us medical technicians, we think; 'Hey, this is working fine. Let's keep it that way'.*"

The installation of updates on medical devices was usually implemented by medical device service technicians, either from the HDO internally or externally from the supplier. Only on rare occasions was it mentioned that clinical users (i.e., nurses, doctors, radiologists) would install any updates. This was even actively avoided in H4, where the central ICT department struggled to disable automatic update pop-ups on certain machines to stay in control of the installation timing. P11-H4 elaborated; "*(...) anybody who starts up the system and gets this message will be allowed to do the update, so we shut that off as much as possible .*"

The decision-making around updating was reported to be more distributed across stakeholders and departments. For regular updates, often the technicians decided independently if and when to install, or would oversee suppliers' external technicians in their updating task. In case the supplier maintained the device, the HDO still had the final say in determining if and when to install updates. The HDO's finance or procurement departments were involved in the decision of which maintenance service contracts to procure (which would determine update frequency and support duration), IT departments would sometimes detect vulnerable devices and demand patches to be installed, and three HDOs had a team of medical physicists responsible for device safety, who would support or oversee technicians in the decision to update. Importantly, the medical departments usually were reported to have the final say and could also demand a particular update. We go into more detail on the decision-making process around updating in subsection 4.3.2.

## 4.2 Patching pathways

To address our first research question (*How are connected medical devices patched within their operational environment at HDOs?*), we provide an overview of the observed different ways in which connected medical devices receive software updates. Based on the interviews with medical device manufacturers and HDOs, we identified four different pathways as to how an available software update, security-related or not, reaches medical devices in the field;

- (i) The manufacturer has a remote connection to the device and can make updates available in this way.
- (ii) Service technicians are sent out by the manufacturer or a certified service supplier, who install updates on-site.
- (iii) The HDO certifies their own technicians, who can, in turn, install updates, which are provided by the manufacturer or supplier.

- (iv) An exploitable vulnerability with a critical risk to patient safety (FDA: "*Uncontrolled risk*") triggers a dedicated emergency update process, in which the patch is to be distributed within a shortened time frame (e.g., according to FDA, within 60 days [26]). This can be achieved by following processes (i), (ii), or (iii). We provide more details on this in Section 4.4.1.

In the following sections, we report on our observations pertaining to (ii), (iii), and (iv), as remote updating was barely reported as a common practice by participating HDOs.

#### 4.2.1 Considerations for choosing a pathway

HDOs differed considerably in their approach to software updates for their medical equipment. Specifically, the level at which the organization managed and installed software updates themselves varied, with some HDOs leaving the majority of updating activities to other parties, while others had their own processes and installed as many updates as possible in their own accordance.

We asked the participants from medical device manufacturers which pathway was most commonly chosen by their customer base. All three manufacturer participants reported that manual installation of software updates by service technicians from them or by third-party service suppliers were the clear majority. P23-M3 estimated this manual installation by service technicians across their products would constitute around 80%.

The ability for manufacturers to make updates available remotely to medical devices was reported to be substantially lower in demand, although being their preferred method, as it allowed them to better control software patching cadence, run remote maintenance and diagnostics, and save on the costly process of dispatching thousands of technicians for a software update. All three manufacturer participants also noted that with increasing size and financial resources, HDOs would be more likely to employ and certify their own technicians to install software patches.

Then, what did the HDOs in our sample say about their considerations as to which update process to choose?

#### 4.2.2 Internal management – drivers

HDOs 1, 4, 8, and 9 ($n = 4$) reported to prefer to have their own technicians install updates on their connected medical devices as much as possible.

A major consideration to keep maintenance and updating in-house was cost. Two HDOs reported it was most financially feasible in the long run instead of opting for a service contract with the supplier. Biomedical technicians usually had to be trained and certified for specific devices to be allowed to maintain the software. Thus, six participants, all technicians at HDOs, regularly attended training for different medical devices, which varied greatly by device (complexity), manufacturer, training scope, length, and required re-certification. Despite high certification costs, both HDOs reported that according to their calculations, maintaining the medical device themselves would still be cheaper.

Another driver to install updates in-house was control of the updating process. P2-H1, P6-H2, and P14-H4, who regularly installed updates on medical devices, stressed the importance for the hospital to control the timing of the update, as devices could not always be removed from service, which then required live monitoring of the device and patient. Instances of uncontrolled updates were given, such as a laptop as part of a medical device automatically initiating an OS update during operations or half a day of canceled patient appointments due to a medical user being prompted on the device UI to install an update, which, unexpected to the user, took several hours.

In fact, control over the installation process was one of the main reasons why HDOs in our sample actively decided against remote and/or automatic software update delivery to their connected medical devices.

#### 4.2.3 External management – drivers

Four other HDOs (ID 2, 5, 6, & 7) reported that for most of their connected medical devices, they would outsource the software maintenance to the supplier via a service contract. This could be the manufacturer, a retailer, or a third-party service supplier.

The most commonly voiced reason for this was medical devices' complexity and safety risks. Four participants explained that for highly complex devices with a potentially difficult and/or dangerous maintenance process, such as those involving strong magnets or radiation, they would keep this process with highly specialized external technicians. This was confirmed from the manufacturer's perspective by P22-M2, who described that for complex devices like an MRI, extensive testing after the installation of an update is required to ensure the absence of any safety risks.

Costs were mentioned as a main consideration again: three participants (P3-H2, P13-H6, & P18-H8) mentioned expensive and re-occurring training and an economy of scale, where it would only be feasible to certify internal technicians if they would have at least a certain volume of devices. Two HDOs also mentioned the benefits of staying within an ecosystem of one manufacturer, which would include updates, but also bulk discounts, and a (relatively) simpler maintenance process.

### 4.3 Patching Connected Medical Devices

To further understand our first research question as well as our second one (*What kind of challenges do HDOs and medical device manufacturers encounter during this process and how are they mitigated?*), we adapt the five-step sequence of Li et al. for the updating process in organizational settings [36], which has been applied in other empirical work on patching practices (e.g., [12, 49]): learning about updates; deciding to update; preparing for installation; deploying updates, and; handling post-update issues.

Naturally, some of the steps differed considerably between HDOs who chose to internalize the updating process and the organizations who outsourced it (most notably in deciding to patch and patch deployment).

#### 4.3.1 Learning about updates

HDO participants reported widely different ways in which they learned about available software updates (including security updates) for their medical devices, especially when compared to conventional IT systems. Most HDOs reported to be in a somewhat passive position and would not proactively check for available updates on a regular basis for all devices. However, there were some differences in this process between HDOs who managed software updates in-house and the ones who outsourced this.

For HDOs managing the software update process for many devices themselves, technicians had to actively check for available updates, as notifications about updates, security-related or not, would not necessarily arrive as a dedicated message but often be posted on a manufacturer-specific web portal, where the technicians could then download it from. In this case, the responsible technician would have to manually check for available updates on the respective platform to decide if the update should be installed.

As most manufacturers were reported to have their own native platform environments and communication methods (e.g., by an updated document, or a dedicated post), this was reported to lead to a considerable burden for medical engineering departments, as the plethora of different platforms and documentations would render active update-tracking extremely time-consuming, approaching impossible, for the entire device base. P10-H4 elaborated; "(...) *we have about 400 different suppliers. I cannot go to all the platforms once a month to check if there's something new.*", with P14-H4 noting "*(...)it's mainly the management process it's not the installation process.*" For this reason, several technicians reported they would check for available updates more or less randomly, whenever they were able to find the time, as they were busy enough with other maintenance duties.

Two HDOs (ID 6 & 8) also reported that email notifications about device updates or emergent risks might at times not follow the defined process, but instead arrive with recipients who would not know what to do with the message, e.g., the medical user who initially purchased the product.

Regarding the actual method of notification, the most commonly mentioned medium across all HDOs was a direct notification (via email or letter) from the manufacturer or the service supplier ($n = 9$), followed by the active checking on manufacturer-native platforms ($n = 4$). Three HDOs (ID 1, 8, & 9) also reported on regular medical device security and/or safety alerts and reports from authorities, such as the Dutch healthcare sector CERT or the MHRA [41] and NHS [44] in the UK, which could refer to an available patch.

More ad-hoc update notification pathways were mentioned across interviews, although less consistently, including; from an external service engineer during their visit, during annual sales/service meetings with manufacturer representatives, or by network surveillance identifying vulnerable medical devices and inquiring about a patch at the manufacturer.

It was less likely to hear from participants that a device's interface would notify them of an update at start-up. Several participants mentioned Log4j in 2021, when involved departments had to actively enquire at manufacturers if their devices would be affected, and when they could expect a fix.

One HDO also reported they would not be notified about available software updates at all. They would install patches on IT infrastructure, but not on connected medical equipment, even though they voiced the desire to control this installed base more actively. "*We know that this seems incredible but with medical devices, manufacturers and suppliers is very difficult to talk to and ask them for [a new software update]*".

#### 4.3.2 Deciding to update

It was often not possible for participants to disentangle security patches from overall software updates, as they would be bundled together. As a result, the decision to update was often made based on non-security aspects such as features, bug fixes, or performance improvements, with security patches as an additional yet less visible part of the update. This was confirmed by all participants from manufacturers, who regarded this as common practice in the sector.

The decision-making of stakeholders at HDOs was thus influenced by other, non-security related factors. "*The (device), it doesn't get security patching, so Windows security patching at all, we leave it as it is. Only when it goes down or when something else is happening, then we think OK, now we can install some patches, but otherwise, we don't install patches on these systems.*" (P2-H1).

Yet, several participants clarified that a dedicated security update without any changes to UI or functionality would just be installed. "*...if it's only (security) patching then uh, the normal process is executed, but if for example also the user interface is changed or settings may be changed, then we perform an additional risk analysis.*" (P3-H2).

Due to the entanglement of updates with functionality, the effort to manage and decide on patching rose considerably for HDOs. Each update had to be assessed for effects on device behavior and interfaces and if a rollback process was in place. For this, considerable communication with other stakeholders was often required, such as asking suppliers for details, checking with medical device safety specialists, and discussing the changes with users; "*And then the medical physicists check* *the release notes. And if there are any user changes, we discuss it with the user. Like you get a new UI or you get a new button somewhere.*"(P11-H4). P10-H4 further explained that getting the necessary release notes for this decision was not always easy: "*We ask for release notes, which are always really difficult to obtain. And there's a lot of companies that still say no release notes.*" This process was potentially multiplied for hundreds of different devices, as for all their software updates, a decision had to be made.

A further struggle and a reason to postpone updates was a complex and time-consuming installation process, from the actual installation to the communication needed with the medical departments. It was often preferred to wait for the next maintenance interval, while several medical technicians also represented the view: "*why disturb something that is working perfectly and create a risk that it is not working perfectly afterward?*" (P2-H1).

Costs played a substantial role here too. Some updates had to be paid for by HDOs. As updates or upgrades (e.g., to a newer OS) would be charged by device, three participants from different HDOs explained how these costs would escalate quickly in case the HDO deployed several devices, and thus being "*not a good business case*" (P3-H2). P14-H4 explained that he would often be asked by his colleagues from IT about why they do not update medical devices more often, to which he would reply "*...because if I install a KB from Microsoft, for the IT guys, just download it, install it, and done. For us, it's paying a bill of 10,000 euros. And then installing it. And then we're done. We have thousands of connected devices, each month, there are updates.*"

Importantly, security-related emergency patches with critical risk were reported to be free of charge, as regulations require manufacturers to respond to such risks if posing a threat to patient safety. However, if the device was running on an outdated OS without patch releases from the OS vendor, only a (paid) upgrade to a newer OS would ensure further security patches. Responsibility for patching is then intertwined: "*In the end, we are responsible to make the final decision that we say yes, it's allowed to patch it, but in a sense... the essence is that the manufacturer or supplier decides this device has to be patched or updated; they have the lead in that process.*" (P3-H2).

### 4.3.3 Preparing for installation

The steps to prepare for installation of an update were mostly related to ensuring continued patient care. This required active communication, and sometimes negotiations, with the medical users of the devices and, if involved, external service technicians, as schedules were usually tight, with many devices running almost 24/7 to maintain patient care: –"*we have to go to every department, ICU the OR and try to arrange this 15 minutes and that takes to a lot of time.*" (P6-H2).

Patching was at times spontaneous and reactive ("*Sometimes we make an appointment with the nurses that they call when the patient is gone and then the guys come with the USB stick*", P13-H6). Conversely, emergency patches installed at short notice could create friction, e.g., telling users; *"Sorry you can't use it now, and tomorrow it'll work. And of course they get mad but not much you can do about it at that time."* (P5-H1). A participant noted that the strain of negotiating with medical departments resulted in the IT department preferring to postpone updates to dedicated maintenance intervals.

The overall sentiment was that medical departments usually understood the need to update and would find a way to install the update, as "*...they know we have to do it.*" (P5-H1). This went as far as scheduling downtime and not booking in patient care that uses a device, "*so (medical staff) know for instance on certain apparatuses they don't have to plan patients because then there is an update.*" (P13-H6).

Testing updates before rollout is a common preparatory step for system administrators of conventional IT systems. [36,49]. For connected medical devices however, HDOs usually did not test the updates before installing them, as this was done by the manufacturer and/or an external supplier. Therefore, several participants also mentioned they would always plan a roll-back process and back-up data before installing updates, to ensure that if the update would introduce any issues, one could go back to the previous version. Subsection 4.3.5 details on post-installation issues.

### 4.3.4 Deploying updates

As depicted in Table 3 (found online[1]) ranging from installing an update every couple of years (e.g., Device 3, 22), to approaching quarterly update cycles (e.g., Device 9, 18). While this corresponds to previous reports and warnings [5, 10, 29, 46], this frequency was reported to be due to costs of updates (be it an effortful and time-consuming process or the actual costs per update) and to the preferred approach to secure medical devices on the network level, which was also done to secure devices running on an outdated OS. "*Medical devices, we do not patch them regularly, most systems. No. No. So we try to have a different approach. We put them in isolated VLANs.*"(P14-H4).

For all update installations reported, physical access to the medical device was needed. This could involve inserting a Flash Drive ($n = 10$), initiating the update via the device's UI ($n = 7$), or via an external Laptop ($n = 6$). Thus, internal and/or external technicians would usually have to go to each device individually to implement and/or oversee the update installation. In one instance for HDO9 (Device 25), it took six months until the external and internal technicians rolled out a firmware update to all 200 ECG devices.

Furthermore, several devices were reported to have dependencies to systems like servers ($n = 7$) , which could lead to dependencies for update installation, such as that updates could be made available to individual devices via a central server, or that installation would have to be done jointly, which, in case of Device 13, would include an external technician coming in with the laptop and update, an internal technician overseeing the process, and a network administrator to take care of the server. Similarly, three HDOs (ID 7, 8, & 9) had a policy in place for some devices (e.g., infusion pumps) that all devices across the organization had to be on the same version to avoid confusion for users. Thus, all devices would have to be updated collectively. Section 4.3.3 details on some of the complexities relating to this process.

Where portable devices (e.g., ultrasounds, automated external defibrillators) could potentially be taken into a workshop, fixed-place devices with intense clinical up-time (e.g., patient monitors, operating room ventilators), would require live (bedsite) monitoring by technicians and nurses during installation: "*We have a policy that we say we want to be at the place when it's done, so we can explain things to to the users.*" (P6-H2).

### 4.3.5 Handling post-update issues

P5-H1 reported he experienced post-installation issues two or three times during his time at the HDO, and in P14-H4's experience, around 5% of software updates would introduce some sort of issue requiring rollback. Several other technicians never experienced this but heard anecdotes about it from their colleagues. Four of the update cases depicted in Table 3[1] were reported to have led to post-update issues and had to be rolled back, for instance, due to unexpected incompatibility with existing hardware (Device 1), or users reporting unexpected device behavior afterward (Device 13, 16, 18).

Preparing for an update only to need to roll back the work was perceived as a very painful process, especially if "*We roll back the update until the manufacturer finds out the cause of the failed update and comes up with a solution.*" (P1-H1).

## 4.4 Manufacturer perspective

We conducted interviews with three product security experts at three large global medical device manufacturers to understand the software update processes across their product portfolio, the risk management and decision-making process prior to security patches, and their observations of what was fed back to them from their customer base. Thus, we could contextualize statements from HDOs and contrast perspectives between these two actors.

### 4.4.1 Security patching processes at manufacturers

The different pathways of software update delivery for connected medical devices offered by manufacturers in our study are described in section 4.2. Participants explained that the release frequency depends on the modality and its OS but that generally, they aimed for regular update package releases (quarterly or bi-yearly), which would usually bundle validated OS, application, and library updates.

In case of an exploitable security vulnerability with patient-safety implications, all three manufacturers had a dedicated process in place to fix devices in the field within a defined timeline. In the medical device sector, such safety-related product warnings and changes after market entry are termed "*Field safety notifications*", and participants estimated this would happen around once or twice per year across their entire product portfolio due to security-related risks.

The manufacturers determined internally if a vulnerability within a medical device and its underlying components required this dedicated patching process. To do so, a risk assessment process was in place at all three manufacturers, in which arising vulnerabilities would be regularly assessed for exploitability and patient safety implications by product security teams using the device's software-bill-of-material (SBOM). Notably, security updates were not the only mitigation option, as the network connections and use context were also considered, which allowed for different mitigation approaches. For instance, P22-M2 explained how an MR residing in a secured room constituted a different security risk than a smaller, mobile, and easily accessible Ultrasound device. Thus, mitigation could also take the form of mandated use, where the manufacturer would mandate the customers to ensure proper protection (e.g., restricting physical access, not connecting it to the Internet, or securing USB ports). Thus, the decision about vulnerabilities' criticality in any soft- or hardware component and the response were decided by the manufacturer on a case-by-case basis, with HDOs then deciding if and when to install any patches resulting from this risk assessment.

In case of regular updates, bundling of security patches with other updates was common practice, although P21-M1 clarified this would depend on the targeted software stack (i.e., dedicated security patches could be released for OS layers).As each change to the system had to ensure continued patient safety under the regulations, validating software updates in test environments was a crucial yet costly process. P21-M1 described a continuous internal balancing and negotiation act, where on the one hand, smaller and dedicated security packages were preferred from a product security perspective due to shorter installation downtime and customers not having to check for functionality changes (and thus, higher install rates), and on the other hand, the push towards reducing costs by validating separate updates together and dispatching technicians for only one bundle.

P21-M1 and P22-M2 stressed that software update delivery for their medical devices was challenging and costly, especially for emergency patches on a shorter time window, as thousands of technicians would have to be dispatched to customers worldwide with their own schedules and infrastructure, and that also for remote software updates, technically implementing a reliable pipeline was non-trivial.

### 4.4.2 Customer observations

We were interested in how manufacturers observed their customers' practices, decisions, and expectations towards software updates and security. As explained in Section 4.2, all three manufacturers observed that patching via a remote connection was in substantially lower demand than manual update delivery via service technicians. In their experience, reasons for this were interrupted schedules when a user would install an update via the device's UI, a dislike for functional changes in updates, a lack of trust towards manufacturers to handle device or patient data appropriately, or the unwillingness to pay for remote updating, as this could also include deploying further infrastructure, such as gateway servers at the hospital site. This mostly overlapped with our findings from HDOs.

They also observed increasingly demanding security and privacy policies from customers the device would have to comply with and a rising demand for more regular and faster patching cycles, especially among customers' IT departments. At the same time, all manufacturers commonly observed their products at HDOs running outdated software and operating systems, thus not being fully patchable, as customers would opt against updating or upgrading the device. P22-M2 explained how instead, many customers would invest in network-based solutions such as micro-segmentation or privileged access management to secure devices, not trusting or not being aware of the security measures implemented into the device itself by the manufacturer.

### 4.4.3 Regulatory ramifications

The majority of regulations for medical device security apply to medical device manufacturers. Thus, the development and maintenance of their products were driven substantially by regulations. While all three participants acknowledged their central role and responsibility for patient safety, they also voiced concerns regarding some regulatory consequences for them and the healthcare sector as a whole.

To comply with all relevant global regulations, their requirements would be mapped to derive a unified process. This required substantial legal and compliance resources and was reported to often lead to a lock-in, where there was limited freedom in design decisions. P22-M2 furthermore explained how this compliance focus could lead to a state where ensuring compliance could put pressure on the communication with customers, who might then fall out of contact with manufacturers and disregard their products' security implementations.

P23-M3 explained how increasing regulatory demands could significantly increase the costs for medical devices and thus healthcare as a whole, as it would require many manufacturers to completely re-design their products' architecture to establish a regular and faster patch delivery process while continuously validating updates. Several HDOs also shared such concerns about the rising costs of medical technology.

## 5 Discussion

In this study, we explored current practices of how connected medical devices receive security patches from the perspective of their operators (HDOs) and manufacturers. We summarize our findings and derive suggestions for practitioners and for future work, yet are cautious to generalize our results or derive categorical recommendations, as this is exploratory work.

### 5.1 Update practices for medical devices

Adressing our first research question (*How are connected medical devices patched within their operational environment at HDOs?*), we identified four different main pathways; Via a remote connection to the manufacturer, manual installation by service engineers, either by the supplier or the HDO, or, in case of vulnerabilities with critical risk, via a field safety notification in a shortened time frame.

We found that HDOs in our sample rarely opted for remote delivery of software updates for their medical devices, even when available, thus requiring manual installation on a per-device level by service technicians. Participants from manufacturers verified this as the most common preference among their customers. This was mainly driven by HDOs' desire to actively control the update process, avoiding interrupted patient care, and concerns for unexpected functional changes in updates.

Instead of having connected medical devices on the latest software version, HDOs often preferred to reduce network exposure, usually by implementing network segments (VLANs) to isolate devices. This was also evidenced by low update install frequencies due to operational overhead and costs for regular updates, thus rendering network solutions more scalable. While this network approach adds an additional security layer and is generally recommended [7, 18, 35], there are also pitfalls. One vulnerable or weakly configured device can compromise the entire segment, which requires active tracking of software versions, vulnerabilities, and configurations of all devices in the segment, which was reportedly not the case in our sample. Previous work investigating HDO networks [15, 35] reported on medical devices frequently residing in the same segment as other IoT or personal devices like IP cameras, printers, or smartphones, defeating the purpose of retaining segments for a single medical use case and increasing risk due to potentially vulnerable IoT devices.

Compared to prior work on patching practices of more conventional IT systems, we identified several key differences in connected medical devices that must be accounted for. Firstly, the stakeholder group of (biomedical) service engineers is responsible for maintaining medical equipment, which includes installing security updates. This is very different from the populations of system administrators and IT professionals studied in other works [3, 14, 24, 36], due to different technical backgrounds and perspectives on IT security. Secondly, while previous work has also identified coordination across actors in the healthcare sector to be crucial in rolling out patches to IT systems [13, 14], our work highlights how connected medical devices, in contrast to backbone IT infrastructure, are significantly more exposed to physical use, thus being potentially mobile and more difficult to access to install patches without interrupting patient care. Thus, patching of medical devices is less scalable and less doable remotely, these being two conditions usually met with conventional IT patching.

Finally, regulations and business practices of the medical device market differ substantially, a topic not broadly covered by previous empirical work. For instance, patching and update support are often part of paid maintenance service contracts, a typical practice in the medical device market, but less so for conventional IT patching. Furthermore, regulations have a stronger effect on patching medical devices than on traditional IT infrastructure, as manufacturers have to validate software updates to their devices to ensure continued safety, which can slow the process and increase costs. While recent work has studied the complex regulatory landscape of medical device security [37], we invite future work to study empirically how current and future regulations (e.g., the PATCH Act [1] or NIS2 [52]) interact with organizational practices of connected medical device security.

### 5.2 Challenges

Previous work identified endpoint complexity [32] and a heterogeneous software updating process [24] for medical devices as major challenges for HDOs' security posture. By asking our second research question (*What kind of challenges do HDOs and medical device manufacturers encounter during this process and how are they mitigated?*), our results provide a more granular view on these challenges from the perspectives of HDOs and manufacturers.

**Costs**. Delivering a software update to medical devices in the field involves substantial costs. It can be an effortful and time-consuming process for HDOs due to non-standardized and heterogeneous notification methods, deciding on complex or incomplete information with mingled security and functional aspects, extensive preparations requiring active communication with medical departments, and a potentially effortful installation process that does not scale well across multiple devices. Furthermore, installing updates usually requires certifications or service contracts for HDOs, and manufacturers need to sustain substantial operational costs for maintenance via service technicians and engage in a continuous validation of updates to keep up with changes across medical devices' hard- and software components.

**Managing infrastructure**. Keeping an overview of and visibility into the installed base of connected medical devices, their software version, active connections, configurations, and available software updates can quickly overwhelm hospitals, especially if they are smaller and/or have limited resources to invest in tools and expertise to manage this. In our study, four of the nine HDOs reported they would attempt to keep up with the changing software versions of medical devices by renewing this in asset management systems after installation, but no HDO had a process in place to proactively and regularly check for available security updates across medical devices and vendors, as this would require substantial additional resources. Instead, even for the largest HDO in our sample, it was perceived as reactive "*firefighting*" (P19-H9) for the involved technical departments due to a lack of resources and strategic vision for proactive management.

**Regulatory implications**. While the global regulatory shift towards more extensive vulnerability management and security patching of connected medical devices (Section 2.3) is promising, our work suggests it poses significant practical challenges for manufacturers and HDOs. More frequent security updates can conflict with the operational reality of many devices, necessitating architectural changes for future devices to enable continuous update validation and delivery while maintaining patient care. Deploying field technicians for each update would not scale with the anticipated increase in patches and device volume. This shift could increase costs for manufacturers, particularly smaller players with less IT experience, potentially reducing market diversity. Newer devices will eventually incorporate such update-delivery pipelines for compliance, but existing 'legacy' devices in circulation will be used for decades, as HDOs (often with limited resources) might run devices without being willing or able to manage patching, given that HDOs have the final say in installing an update while regulations predominantly target manufacturers regarding product security.

**Entrenched silos**. Medical devices' growing connectivity increasingly merges medical engineering (safety, functionality, usability) and IT (network connectivity, software, security). We observed this coupling of different disciplines raising challenges for both HDOs and manufacturers, such as differing priorities and expectations, even if combined structurally as departments. As IT staff expected frequent patches and control over the medical devices like for any other IT system, clinical engineers were more reluctant to change a functional system. For manufacturers, different priorities between security and features can constitute a balancing act.

Several of our identified challenges are congruent with previous work on security updates from other domains like consumer IoT or organizational IT, such as the potential for update-induced bugs, unexpected functional changes, or difficulty in obtaining all necessary patch information, e.g., due to a lack of a centralized source or release notes [11, 16, 25, 33, 36, 49, 53]. We extend this work to connected medical devices, identifying challenges unique to this domain, such as difficulties in locating and accessing physical devices despite intense medical use and the need to define responsibilities across clinical engineering and IT stakeholders.

### 5.3 Limitations

Our research has several limitations. Firstly, the samples of HDOs, medical device manufacturers, and patch cases do not necessarily represent the general population. Participants noted country differences in medical device security and patching, suggesting future research opportunities. Furthermore, due to the smaller sample of manufacturers, we did not reach full theoretical saturation for these three interviews. Still, they are large, globally-active market players reaching thousands of HDOs. Thus, our results provide valuable insights into the centralized risk and vulnerability management processes and experiences with customers worldwide.

We relied on a convenience sample from a hard-to-reach expert population in a strained healthcare sector, which may have led to self-selection bias [30], as organizations more adept at the security of medical technology might have been more likely to participate. Furthermore, the sampled patching cases during the interviews were based on participants' retrospective memory, potentially affecting some claims. However, we structured those recollections to facilitate comparison between HDOs and devices, albeit based on estimates rather than verified numbers.

Lastly, four interviews included multiple participants (see Section 3.3), potentially introducing bias like groupthink or reluctance to speak freely. This format was suggested by participants however, signaling a willingness to share experiences in a group setting. During the interview, the interviewer also adhered closely to the protocol and directed questions to each participant to keep interviews comparable. Questions were answered directly by one participant, occasionally supplemented by another; this represented how answers to complex problems may require the expertise of multiple professionals.

### 5.4 Recommendations

**Managing updates at HDOs:** To reduce HDOs' burden to manage software updates, a structured process to evaluate available updates was reported to be essential. For instance, HDO4 defined a role (in this case, medical physicists) to evaluate or demand the necessary update details and had a check-list that was iterated over for each software update; this helped structure the decision and clarify which aspects of an update need to be discussed with whom. Channeling all communications with vendors regarding safety and security through one contact (e.g., one email address or one department), helped HDO8 to streamline communications. Manufacturers should support HDOs in navigating the complexities of varying notification channels and formats of available updates or vulnerabilities by standardizing them together with other vendors, which would reduce the burden for HDOs and thus lead to higher install rates. As seen in our results, SBOMs furthermore help manufacturers to render the complexity of a medical device and its components manageable [6] and deliver more specific alerts to customers, if need be.

**Interdisciplinary collaboration:** Due to the increasing entanglement of hard- and software-related responsibilities regarding connected medical devices, we also want to highlight to HDOs the need for close collaboration between departments. Initiating dedicated commissions, projects, or clusters between IT, medical engineering, governance, and/or procurement departments helped HDOs in our study to manage both hard- and software-related challenges and uncertainties by bundling the necessary expertise. Importantly, we found that merging departments did not necessarily result in more effective cooperation due to vastly different approaches, tools, and cultures. Instead, we recommend HDOs to acknowledge the different worlds of IT and medical engineering but establish structures that allow for mutual, regular cooperation and bilateral learning to improve the capabilities to manage the increasing connectivity of medical technology.

**Non-disruptive update mechanisms:** We found that a major reason for HDOs to avoid remote updating, which could enable regular security patches, was the loss of control over the installation process and potential disruptions to patient care, as well as potential distrust towards the manufacturer. Thus, providing remote update methods that retain control over the installation for HDOs could increase adoption rates and trust towards updates and manufacturers. Case studies [55] and guidelines [18, 19] provide insights into how a continuous patch delivery process can be deployed that allows for operators' flexibility to install. Yet, if costs for such a deployment exceed manual software installations via service technicians, HDOs will have less incentive to opt for it.

## 6 Conclusion

In this work, we studied organizational practices surrounding the security patching of connected medical devices in their operational environment at HDOs. We found that providing such systems with security updates is non-trivial for the involved actors due to challenges in tracking software attributes across a vast and heterogeneous inventory of medical devices, an increasing strain for technical departments at HDOs to manage this infrastructure, and practical difficulties in preparing for and actually installing updates amidst medical use, as this usually required physical access to each device.

While medical devices become increasingly connected and are exposed to an evolving threat landscape, new regulations push towards a more frequent and faster delivery of security patches for such systems. Our work highlights that patching comes at a cost however, as dispatching and/or certifying technicians to install updates did not scale well and that willingness among HDOs to adopt available remote updating capabilities for medical devices was low. It thus remains to be seen how the actors in the healthcare system will balance such regulatory requirements with upcoming costs and medical device security and, thus, patient safety.

## Acknowledgments

This research was partly funded by the Dutch Research Council (NWO) via project THESEUS (Grant nr. NWA.1215.18.006) and INTERSCT (Grant nr. NWA.1160.18.301). We want to thank everyone who took the time to participate in this study, the practitioners who helped us with reaching out to potential participants, as well as the shepherd and reviewers for their valuable feedback.

## References

[1] S.3983 - 117th Congress (2021-2022). PATCH Act, S.3983, 2022. URL: https://www.congress.gov/bill/117th-congress/senate-bill/3983.

[2] Chon Abraham, Dave Chatterjee, and Ronald R. Sims. Muddling through cybersecurity: Insights from the U.S. healthcare industry. *Business Horizons*, 62(4):539–548, July 2019. URL: https://www.sciencedirect.com/science/article/pii/S0007681319300436, doi:10.1016/j.bushor.2019.03.010.

[3] Tamara Bondar, Hala Assal, and AbdelRahman Abdou. Why do Internet Devices Remain Vulnerable? A Survey with System Administrators. *NDSS Symposium*, 2023. URL: https://www.ndss-symposium.org/ndss-paper/auto-draft-421/.

[4] Virginia Braun and Victoria Clarke. One size fits all? What counts as quality practice in (reflexive) thematic analysis? *Qualitative research in psychology*, 18(3):328–352, 2021.

[5] Zach Capers. More Healthcare Devices Means More Cyberattacks — How Weak Medical IoT Security Threatens Patient Care, November 2022. URL: https://www.capterra.com/resources/medical-internet-of-things-iot-security/.

[6] Seth Carmody, Andrea Coravos, Ginny Fahs, Audra Hatch, Janine Medina, Beau Woods, and Joshua Corman. Building resilient medical technology supply chains with a software bill of materials. *npj Digital Medicine*, 4(1):1–6, February 2021. Number: 1 Publisher: Nature Publishing Group. doi:10.1038/s41746-021-00403-w.

[7] Ramaswamy Chandramouli. Guide to a Secure Enterprise Network Landscape. *NIST Special Publication*, 2022.

[8] Lynne Coventry and Dawn Branley. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, 113:48–52, July 2018. doi:10.1016/j.maturitas.2018.04.008.

[9] Lynne Coventry, Dawn Branley-Bell, Elizabeth Sillence, Sabina Magalini, Pasquale Mari, Aimilia Magkanaraki, and Kalliopi Anastasopoulou. Cyber-Risk in Healthcare: Exploring Facilitators and Barriers to Secure Behaviour. In *International conference on human-computer interaction*, pages 105–122. Springer International Publishing, 2020. doi:10.1007/978-3-030-50309-3_8.

[10] Cynerio. Cynerio Research Finds Critical Medical Device Risks Continue to Threaten Hospital Security and Patient Safety, 2022. URL: https://www.cynerio.com/blog/cynerio-research-finds-critical-medical-device-risks-continue-to-threaten-hospital-security-and-patient-safety.

[11] Nesara Dissanayake, Asangi Jayatilaka, Mansooreh Zahedi, and M. Ali Babar. Software security patch management - A systematic literature review of challenges, approaches, tools and practices. *Information and Software Technology*, 144:106771, April 2022. doi:10.1016/j.infsof.2021.106771.

[12] Nesara Dissanayake, Asangi Jayatilaka, Mansooreh Zahedi, and Muhammad Ali Babar. An Empirical Study of Automation in Software Security Patch Management. In *Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering*, ASE '22, pages 1–13. Association for Computing Machinery, January 2023. doi:10.1145/3551349.3556969.

[13] Nesara Dissanayake, Mansooreh Zahedi, Asangi Jayatilaka, and Muhammad Ali Babar. A grounded theory of the role of coordination in software security patch management. In *Proceedings of the 29th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, ESEC/FSE 2021, pages 793–805. Association for Computing Machinery, August 2021. doi:10.1145/3468264.3468595.

[14] Nesara Dissanayake, Mansooreh Zahedi, Asangi Jayatilaka, and Muhammad Ali Babar. Why, How and Where of Delays in Software Security Patch Management: An Empirical Investigation in the Healthcare Sector. *Proceedings of the ACM on Human-Computer Interaction*, 6(CSCW2):362:1–362:29, November 2022. doi:10.1145/3555087.

[15] Guillaume Dupont, Daniel Ricardo dos Santos, Elisa Costante, Jerry den Hartog, and Sandro Etalle. A Matter of Life and Death: Analyzing the Security of Healthcare Networks. In *ICT Systems Security and Privacy Protection*, IFIP Advances in Information and Communication Technology, pages 355–369, Cham, 2020. Springer International Publishing. doi:10.1007/978-3-030-58201-2_24.

[16] Sadegh Farhang, Jake Weidman, Mohammad Mahdi Kamani, Jens Grossklags, and Peng Liu. Take It or Leave It: A Survey Study on Operating System Upgrade Practices. In *Proceedings of the 34th Annual Computer Security Applications Conference*, ACSAC '18, pages 490–504, New York, NY, USA, December 2018. Association for Computing Machinery. doi:10.1145/3274694.3274733.

[17] Jean Faugier and Mary Sargeant. Sampling hard to reach populations. *Journal of advanced nursing*, 26(4):790–797, 1997.

[18] International Medical Device Regulators Forum. Principles and Practices for Medical Device Cybersecurity, April 2020. URL: https://www.imdrf.org/documents/principles-and-practices-medical-device-cybersecurity.

[19] International Medical Device Regulators Forum. Principles and Practices for the Cybersecurity of Legacy Medical Devices, April 2023. URL: https://www.imdrf.org/documents/principles-and-practices-cybersecurity-legacy-medical-devices.

[20] Leo A Goodman. Snowball sampling. *The annals of mathematical statistics*, pages 148–170, 1961.

[21] Government of the United Kingdom. The Medical Devices Regulations 2002 (SI 2002/618), 2002. URL: https://www.legislation.gov.uk/uksi/2002/618/contents/made.

[22] Ames Gross. Japan Outlines New Medical Device Cybersecurity Regulation, 2023. URL: https://www.pacificbridgemedical.com/news-brief/japan-outlines-new-medical-device-cybersecurity-regulation/.

[23] Greg Guest, Arwen Bunce, and Laura Johnson. How Many Interviews Are Enough?: An Experiment with Data Saturation and Variability. *Field methods*, 18(1):59–82, 2006. doi:10.1177/1525822X05279903.

[24] Marco Gutfleisch, Markus Schöps, Jonas Hielscher, Mary Cheney, Sibel Sayin, Nathalie Schuhmacher, Ali Mohamad, and M. Angela Sasse. Caring About IoT-Security – An Interview Study in the Healthcare Sector. In *Proceedings of the 2022 European Symposium on Usable Security*, EuroUSEC '22, pages 202–215. Association for Computing Machinery, 2022. doi:10.1145/3549015.3554209.

[25] Julie M Haney and Susanne M Furman. User Perceptions and Experiences with Smart Home Updates. In *2023 IEEE Symposium on Security and Privacy (SP)*, pages 2867–2884. IEEE, 2023. doi:10.1109/SP46215.2023.10179459.

[26] Center for Devices and Radiological Health. Postmarket Management of Cybersecurity in Medical Devices. *U.S. Food and Drug Administration*, December 2016. URL: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices.

[27] Center for Devices and Radiological Health. Cybersecurity in Medical Devices: Refuse to Accept Policy for Cyber Devices and Related Systems Under Section 524B of the FD&C Act. *U.S. Food and Drug Administration*, March 2023. URL: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-refuse-accept-policy-cyber-devices-and-related-systems-under-section.

[28] Center for Devices and Radiological Health and Center for Biologics Evaluation and Research. Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions. *U.S. Food and Drug Administration*, April 2022. URL: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions.

[29] Securin Health-ISAC, Finite State. Exploitable Vulnerabilities That Expose Healthcare Facilities Surged Nearly 60% Since 2022, New Research Report Finds. *Health-ISAC - Health Information Sharing and Analysis Center*, August 2023. URL: https://h-isac.org/2023-state-of-cybersecurity-for-medical-devices-and-healthcare-systems/.

[30] James J Heckman. Selection Bias and Self-selection. In *Econometrics*, pages 201–224. Springer, 1990.

[31] International Electrotechnical Commission (IEC). IEC 81001-5-1:2021, 2021. URL: https://www.iso.org/standard/76097.html.

[32] Mohammad S. Jalali and Jessica P. Kaiser. Cybersecurity in Hospitals: A Systematic, Organizational Perspective. *Journal of Medical Internet Research*, 20(5):e10059, 2018. doi:10.2196/10059.

[33] Adam Jenkins, Pieris Kalligeros, Kami Vaniea, and Maria K Wolters. "Anyone Else Seeing this Error?": Community, System Administrators, and Patch Information. In *2020 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 105–119. IEEE, 2020.

[34] Ross Koppel, Sean Smith, Jim Blythe, and Vijay Kothari. Workarounds to Computer Access in Healthcare Organizations: You Want My Password or a Dead Patient? In *Driving Quality in Informatics: Fulfilling the Promise*, pages 215–220. IOS Press, 2015. doi:10.3233/978-1-61499-488-6-215.

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

[36] Frank Li, Lisa Rogers, Arunesh Mathur, Nathan Malkin, and Marshini Chetty. Keepers of the Machines: Examining How System Administrators Manage Software Updates For Multiple Machines. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 273–288, 2019.

[37] Kaspar Rosager Ludvigsen. The Role of Cybersecurity in Medical Devices Regulation: Future Considerations and Solutions. *Law, Technology and Humans*, 5(2):59–77, November 2023. doi:10.5204/lthj.3080.

[38] Arunesh Mathur, Nathan Malkin, Marian Harbach, Eyal Peer, and Serge Egelman. Quantifying Users' Beliefs about Software Updates. In *NDSS Workshop on Usable Security*, 2018. doi:10.14722/usec.2018.23036.

[39] Emma McMahon, Ryan Williams, Malaka El, Sagar Samtani, Mark Patton, and Hsinchun Chen. Assessing medical device vulnerabilities on the Internet of Things. In *2017 IEEE International Conference on Intelligence and Security Informatics (ISI)*, pages 176–178, July 2017. doi:10.1109/ISI.2017.8004903.

[40] Sharan B. Merriam and Elizabeth J. Tisdell. *Qualitative Research: A Guide to Design and Implementation*. John Wiley & Sons, August 2015.

[41] MHRA. Alerts, recalls and safety information: drugs and medical devices. URL: https://www.gov.uk/drug-device-alerts?alert_type%5B%5D=field-safety-notices.

[42] MHRA. Implementation of the Future Regulations, 2024. URL: https://www.gov.uk/government/publications/implementation-of-the-future-regulation-of-medical-devices/implementation-of-the-future-regulations.

[43] Yisroel Mirsky, Tom Mahler, Ilan Shelef, and Yuval Elovici. CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning. In *USENIX Security Symposium*, volume 2019, 2019.

[44] NHS. Cyber alerts. URL: https://digital.nhs.uk/cyber-alerts.

[45] NHS. Cyber security guidance for healthcare professionals procuring and deploying connected medical devices. URL: https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/guidance-for-procuring-and-deploying-connected-medical-devices.

[46] Federal Bureau of Investigation. Unpatched and Outdated Medical Devices Provide Cyber Attack Opportunities, September 2022. URL: https://www.aha.org/system/files/media/file/2022/09/fbi-pin-tlp-white-unpatched-and-outdated-medical-devices-provide-cyber-attack-opportunities-sept-12-2022.pdf.

[47] Morgen E. Peck. Medical Devices Are Vulnerable to Hacks, But Risk Is Low Overall - IEEE Spectrum, 2011. URL: https://spectrum.ieee.org/medical-devices-are-vulnerable-to-hacks-but-risk-is-low-overall.

[48] Elizabeth Stobert, David Barrera, Valérie Homier, and Daniel Kollek. Understanding Cybersecurity Practices in Emergency Departments. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20, pages 1–8, New York, NY, USA, April 2020. Association for Computing Machinery. doi:10.1145/3313831.3376881.

[49] Christian Tiefenau, Maximilian Häring, Katharina Krombholz, and Emanuel von Zezschwitz. Security, Availability, and Multiple Information Sources: Exploring Update Behavior of System Administrators. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*, pages 239–258, 2020. URL: https://www.usenix.org/conference/soups2020/presentation/tiefenau.

[50] European Union. 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). *Official Journal*, 2016. URL: http://data.europa.eu/eli/reg/2016/679/2016-05-04.

[51] European Union. 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. *Official Journal*, 2017. URL: http://data.europa.eu/eli/reg/2017/745/2023-03-20.

[52] European Union. 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). *Official Journal*, 2022. URL: http://data.europa.eu/eli/dir/2022/2555/oj.

[53] Kami Vaniea and Yasmeen Rashidi. Tales of Software Updates: The process of updating software. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 3215–3226. ACM, May 2016. doi:10.1145/2858036.2858303.

[54] Luis Vargas, Logan Blue, Vanessa Frost, Christopher Patton, Nolen Scaife, Kevin RB Butler, and Patrick Traynor. Digital Healthcare-Associated Infection: A Case Study on the Security of a Major Multi-Campus Hospital System. In *NDSS*, 2019.

[55] Hans-Martin von Stockhausen and Marc Rose. Continuous security patch delivery and risk management for medical devices. In *2020 IEEE International Conference on Software Architecture Companion (ICSA-C)*, pages 204–209. IEEE, 2020.

[56] Markus Willing, Christian Dresen, Eva Gerlitz, Maximilian Haering, Matthew Smith, Carmen Binnewies, Tim Guess, Uwe Haverkamp, and Sebastian Schinzel. Behavioral responses to a cyber attack in a hospital environment. *Scientific Reports*, 11(1):19352, September 2021. Number: 1 Publisher: Nature Publishing Group. doi:10.1038/s41598-021-98576-7.

# A Appendix

**Healthcare Delivery Organization participants:**

| PID | HDO ID | Country | Role | Department | # cases | Experience |
|---|---|---|---|---|---|---|
| 1 | 1 | NL | Network Admin | ICT | - | Prefer not to say |
| 2 | 1 | NL | Biomedical Engineer | Medical Engineering | 3 | 15 - 19 years |
| 3 | 2 | NL | Medical Physicist | Medical Engineering | - | 10 - 14 years |
| 4 | 2 | NL | Security Officer | IT | - | 1 - 4 years |
| 5 | 1 | NL | Biomedical Engineer | Medical Engineering | 3 | 5 - 9 years |
| 6 | 2 | NL | Biomedical Engineer | Medical Engineering | 1 | 15 - 19 years |
| 7 | 3 | ITA | IT/ICT Manager | ICT | - | 15 - 19 years |
| 8 | 3 | ITA | Biomedical Engineer | Medical Engineering | - | $<$ 1 year |
| 9 | 3 | ITA | System Admin | IT | - | $\geq$ 20 years |
| 10 | 4 | NL | Medical Physicist | M-ICT department | - | $\geq$ 20 years |
| 11 | 4 | NL | Biomedical Engineer | M-ICT department | 3 | 15 - 19 years |
| 12 | 5 | NL | Biomedical Engineer | Medical Engineering | 1 | 15 - 19 years |
| 13 | 6 | NL | Medical Physicist | Medical Physics | 3 | $\geq$ 20 years |
| 14 | 4 | NL | Biomedical Engineer | M-ICT department | 3 | 5 - 9 years |
| 15 | 6 | NL | Biomedical Engineer | Medical Technology | - | $\geq$ 20 years |
| 16 | 6 | NL | Biomedical Engineer | Medical Technology | 3 | $\geq$ 20 years |
| 17 | 7 | NL | Biomedical Engineer | Medical Technology | 3 | $\geq$ 20 years |
| 18 | 8 | UK | Biomedical Engineer | Clinical Engineering | 1 | $<$ 1 year |
| 19 | 9 | UK | Biomedical Engineer | Clinical Engineering | 1 | 1 - 4 years |
| 20 | 9 | UK | Biomedical Engineer | Clinical Engineering | 1 | 1 - 4 years |

**Medical Device Manufacturer participants:**

| PID | Manu. ID | Country | Role | Department | Experience |
|---|---|---|---|---|---|
| 21 | 1 | DE | Product Security Specialist | Corporate Cybersecurity | 10 - 14 years |
| 22 | 2 | NL | Product Security Specialist | Product Security | 1 - 4 years |
| 23 | 3 | DE | Product Security Specialist | Product Management | 1 - 4 years |

Table 2: Participants' demographics. **# cases** indicates how many patch cases were mentioned during the interview. In case none were provided, the role did not implement software updates themselves. **Experience** refers to time in this role. For privacy reasons, role names were generalized.