Caring About IoT-Security – An Interview Study in the Healthcare Sector

Marco Gutfleisch
Ruhr University Bochum, Germany
marco.gutfleisch@rub.de

Markus Schöps
Ruhr University Bochum, Germany
markus.schoeps@rub.de

Jonas Hielscher
Ruhr University Bochum, Germany
jonas.hielscher@rub.de

Mary Cheney
Ruhr University Bochum, Germany
mary.cheney@rub.de

Sibel Sayin
Ruhr University Bochum, Germany
sibel.sayin@rub.de

Nathalie Schuhmacher
Ruhr University Bochum, Germany
nathalie.schuhmacher@rub.de

Ali Mohamad
Ruhr University Bochum, Germany
ali.mohamad@rub.de

M. Angela Sasse
Ruhr University Bochum, Germany
angela.sasse@rub.de

ABSTRACT

The number of medical IoT devices is increasing rapidly: CT scanners, ECG devices, insulin pumps and other devices, which previously operated independently, are being interconnected with other devices, now sharing patient data and/or uploading them to the cloud. Medical IoT devices can create privacy and security risks for patients, healthcare professionals, and the institutions that deploy them. Previous security research has focused on software vulnerabilities in IoT devices, and how they could be exploited. This study takes a broader security perspective, looking at security issues that arise in the life cycle of IoT devices deployed in healthcare environments. We performed in-depth online interviews lasting over 1 hour (12 hours in total) with $n = 8$ experts responsible for the security of medical IoT devices in hospitals. They had on average 20 years of industry experience (IT and/or security), and spoke from the experience of either in-hospital specialist, or as external consultants that advise multiple hospitals on IT security. Our findings suggest that medical IoT devices are a security time bomb: the inability to easily patch devices due to certification regulations, the requirements of manufacturers to enable remote maintenance, and the lack of qualified personnel and resources result in low levels of security, even compared to general IT systems in hospitals (which have been found to be vulnerable due to age and lack of security expertise). More encouragingly, most participants reported that awareness of hospital managers & manufacturers of these issues has improved, following new legislation on IT security in hospitals in Germany and the EU over the last two years. We conclude that the security and privacy risks of medical IoT devices is currently underestimated, and that a collaborative effort with manufacturers and primary users (medical staff) will be required to create effective processes for securing them.

EuroUSEC 2022, September 29–30, 2022, Karlsruhe, Germany

ACM ISBN 978-1-4503-9700-1/22/09.
https://doi.org/10.1145/3549015.3554209

KEYWORDS

Healthcare IT Security, Human-Centred Security, Interview Study, IoT Security

ACM Reference Format:
Marco Gutfleisch, Markus Schöps, Jonas Hielscher, Mary Cheney, Sibel Sayin, Nathalie Schuhmacher, Ali Mohamad, and M. Angela Sasse. 2022. Caring About IoT-Security – An Interview Study in the Healthcare Sector. In *2022 European Symposium on Usable Security (EuroUSEC 2022), September 29–30, 2022, Karlsruhe, Germany*. ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3549015.3554209

1 INTRODUCTION

Internet of Things (IoT) devices are increasingly used in work and home settings. The healthcare sector is one example where devices are rapidly "going IoT" from individual devices (implants, respirators, infusion and insulin pumps) to larger equipment (such as CT scanners and ECG monitors) [59]. These devices can connect and communicate with each other, as well as external entities (e.g. their manufacturers), thus creating a complex system of interconnected devices that can automatize processes like data analysis and evaluation [51]. The security of healthcare IoT devices is critical to patient safety. As part of Project 392 "Manipulation of medical devices (ManiMed)", the German Federal Office for Information Security (BSI) conducted an IT security assessment of ten relevant interconnected medical devices to showcase the current state of IoT security in healthcare and raise awareness of potential security challenges [59]. Over 150 security vulnerabilities, primarily within the accompanying infrastructure of the IoT devices, were identified. Many of of these vulnerabilities are unintentional - absent or weak access control and design and implementation and configuration errors may occur because the manufacturers or component suppliers do not follow secure development practices [13]. In one prominent case, vulnerabilities that could have impacted children's privacy and safety were found in a toy doll [10]. Some vulnerabilities identified are suspected to have been intentional, to enable access to data from deployed devices.

This study aimed to investigate the extent to which privacy and security issues associated with medical IoT devices exist and what security practices are currently implemented. We interviewed IT professionals who have worked in the healthcare sector about the

challenges they have experienced in relation to IoT devices, and how they have managed them during at different stages (procurement, integration, maintenance and in use). We decided to specifically ask IT professionals in hospitals because they have a broader understanding of security and privacy challenges in this environment, and are best suited to identify the new challenges that these devices create. We consider every connected medical device as a medical IoT device, and focused on the following research question:

RQ: What factors impact security in the later stages of the lifecycle of IoT devices used in the professional healthcare sector (in procurement, integration & maintenance and during the usage)?

2 RELATED WORK & BACKGROUND

There is a growing body of related work on IoT benefits and security issues.

2.1 IoT: Applications and Benefits

IoT technology has been implemented in various sectors: retail [12], smart transportation [62], agriculture [22], healthcare [30] and others [57]. IoT-based healthcare systems can provide enhanced monitoring of patients' health, deliver treatment in a more targeted way, and provide centralized electronic storage of patient records. Centralized storage allows healthcare providers to access those records whenever it is needed, irrespective of where data was initially recorded, and enables more efficient analysis of patient data [4, 16]. Such systems also improve evaluation of patient data and reduce the chances of significant developments in patient health being missed, because regular automated analyses of the data can identify major shifts, or actionable test results that are sometimes missed by physicians [15, 32]. IoT devices like context motion tracking and Implantable Medical Devices also allow for continuous remote health monitoring [48, 49], which is especially beneficial for chronically ill patients [34, 48]. The devices offer early detection of possible medical issues or emergency situations, and generally improve quality of life for those patients. The storage, processing and analysis of health data can be made more efficient and accessible using mobile health applications that transmit data to cloud servers [21, 38, 48]. There is also a financial advantage in using IoT-enabled devices by allowing patients to monitor their own health status and consult doctors only when necessary, reducing costly emergency room visits and hospitalizations [21, 24].

2.2 Usable Security

Usable security refers to security measures that account for the human factors involved – a device or network's security must be compatible with the behaviors of anyone using it, and thus effectively integrated into the community it is designed for [35, 54]. In the context of healthcare, there are two sides to usability: (1) healthcare professionals (doctors, nurses, therapists, etc.) and (2) patients [39]. Some approaches to increasing security usability include automation (implementing security measures that do not require user intervention), developing user interfaces based on with users' mental models, and teaching users about security risks and correct security practices [14, 61]. The latter in particular is widely practiced, with billions of $ being spent globally on security awareness campaigns and training, yet they are largely ineffective [7] Sasse et al., highlight that security awareness campaigns in the healthcare sector often only warn of risks and exhort staff to "be aware", but lack concrete instructions on secure behaviours[55]. A common misconception is that increasing usability lowers security, but the fact is that unusable security is never effective, because users do not adopt it, and/or make mistakes even when they try [25, 50]. This challenge is amplified in the healthcare sector because time to access medical devices is critical to effective treatment, so cumbersome security measures can put lives at risk [11, 63]

2.3 Laws & Regulations

The German *Medical Devices Act* (German: *Medizinproduktegesetz*, short: MPG) regulates what devices are approved for use in healthcare, and provides requirements for their handling [17]. Most diagnostic tools and treatment units found in hospitals fall under this act – including medical IoT devices. Before a device receives approval under the MPG, it undergoes a long certification process that scrutinizes both hardware and software. All changes to the device, including the software, usually have to be re-certified. The MPG also requires a party to be designated responsible for each product (in most cases, this is the manufacturer). For every medical IoT device this responsible party has to create a risk analysis, including every network interface. In the MPG's most recent revision in 2020, multiple IT security specific requirements were added, such as that manufacturers have to develop software to ensure the proper functioning of the medical device. Most hospitals in Germany are considered critical infrastructure, thus fall under the *KRITIS act* [18]. As such, hospitals must report all major IT security incidents, so that members of the public - including current or potential patients - can check the number and severity of IT security incidents in a hospital. (Public and private sector organisations in Germany that are not KRITIS are not required to report such incidents.) All German hospitals are also required to report any security and privacy incident that affect user (patient) data, under the legislation of the EU GDPR. The 2020 *Hospital Futures Act* (German: *Krankenhauszukunftsgesetz*, short: KHZG) dedicates substantial funding from the federal government to improve IT security standards in German hospitals [19].

2.4 Known Problems Regarding IoT in the Healthcare Sector

Security and Data Privacy. IoT devices have been shown to contain vulnerabilities that can be exploited by attackers or other unauthorized users[5, 56] and potentially jeopardize patient safety [45]. For example, wireless insulin pumps used by diabetic patients can be remotely manipulated, e.g. to deliver a fatal overdose [23, 27]. Patients can also be victims of identity theft if hackers exploit sensitive patient data to create a fake ID [1], for instance, to obtain medication for resale [2]. Whilst in IT security such risks are often managed by making users aware and proscribing certain behaviours, IoT data can be attacked at any stage - from the device to the network to the cloud [21, 40].

Trust. [31, 51] Medical professionals and patients report reluctance or even unwillingness to use medical IoT devices, due to

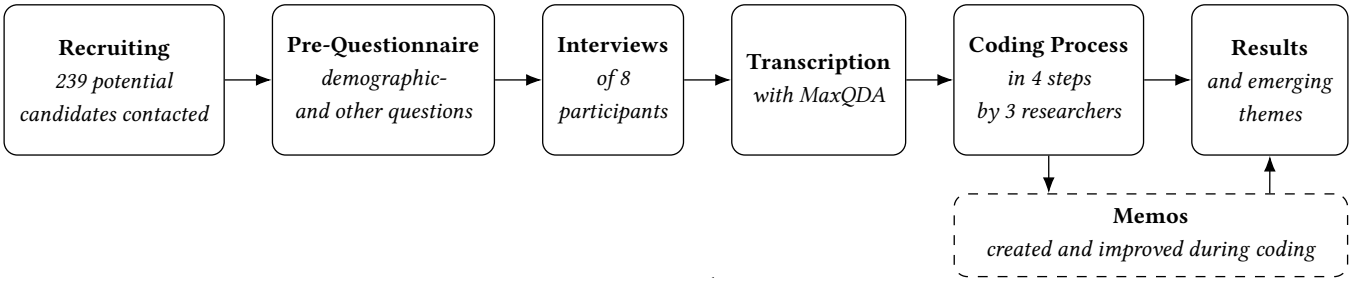

Figure 1: Study procedure.

low trust in their functionality and the accuracy of the transmitted medical data. Hui et al. [29] interviewed a total of 12 patients and 12 clinicians about their perceived trust in medical IoT devices, and report patients had low confidence that the system could operate without disruption and errors.

Interoperability. IoT devices' ability to connect and communicate with each other is not a given, but must be actively ensured during manufacturing which is challenging due to lacking and changing standards and technology as well as cost constraints [51]. Poor interoperability complicates the management and integration of large amounts of heterogeneous data [42, 46].

Data Quality. Good medical decisions need high-quality data, i.e. that is "fit for use" [58] and fulfills certain criteria including accuracy, validity, timeliness, and completeness [41]. Data collected and transmitted via IoT technology always bears the risk of being inaccurate or incomplete due to noise, data leakage and outliers [3, 6]. This can lead to interpretation errors and poor treatment choices.

3 METHODOLOGY

We conducted eight interviews with highly experienced IT professionals from the healthcare sector. Prior to interviews, all participants filled out a pre-questionnaire for demographic data collection and scheduling purposes. Our study process is illustrated in figure 1. In section 3.1 we describe how we developed, piloted and structured the interview guide and the pre-questionnaire. The following sections discuss participant recruitment (3.2), the analysis process (3.3) and study ethics/data protection (3.4).

3.1 Interview Guide & Procedure

In this section we describe the development of the interview guide, the interview guide's structure and the interview procedure. The final interview guide and pre-questionnaire can be found in the appendix (B).

Instrument Development. The interview guide was created in multiple steps. First, five researchers collected candidate interview questions to elicit the information required to answer our research question. From the candidate questions, three researchers made an initial selection of the most applicable questions during collaborative sessions. Those questions were then categorised and similar questions were removed. We wanted participants to discuss specific examples from their careers and further guide participants through the different stages of the IoT life cycle. As categories fully emerged, we added additional questions that helped gain a deeper understanding of a participant's real-life example. We piloted the interview guide with one participant from the professional healthcare sector. We did not make any subsequent changes and, as our pilot candidate satisfied recruiting criteria, we included this participant in our final sample.

Pre-Questionnaire. All demographic and other quantitative questions were included in the pre-questionnaire filled out by participants prior to each interview for the purpose of conserving time. The questionnaire also included a date scheduling feature to make scheduling the interview easy for participants. We also provided an online and downloadable version of our consent form at the beginning of the questionnaire.

Interview Guide Structure. The interview guide started with a short warm-up phase, in which we resolved any of the participant's queries regarding data protection or the interview in general. The remaining guide is divided into five categories: The first three (*Procurement, Integration & Maintenance, Usage*) aim to guide the participant through various stages of the IoT life cycle. The next category (*Attitudes*) contains questions that focus on the participants' opinions of, attitudes towards, and hopes for the interplay between usability and security as well as security related to medical IoT devices. Finally, the interview guide contains two last questions asking whether the participant has anything to add or would like to discuss a specific topic to conclude the interview. The full interview guide can be found in appendix (B).

Interview Procedure. We sent a link to the pre-questionnaire to interested participants. The first part of the pre-questionnaire provided information about the research institute, participant rights and how participant data would be handled. After answering demographic questions, participants could select a desired interview date. At the time of the interview we first answered any questions about the consent form and addressed any concerns or discomforts. We used a common video conference tool for all interviews and captured all audio tracks locally on the interviewer's machine. Seven interviews were conducted in German and one in English. All interviews were conducted by the same researcher.

3.2 Recruiting

We wanted to recruit IT professionals with insights into the problems and challenges in the professional healthcare sector. We recruited participants who work(ed) either as IT professionals in hospitals or as IT consultants for hospitals. We recruited via e-mail,

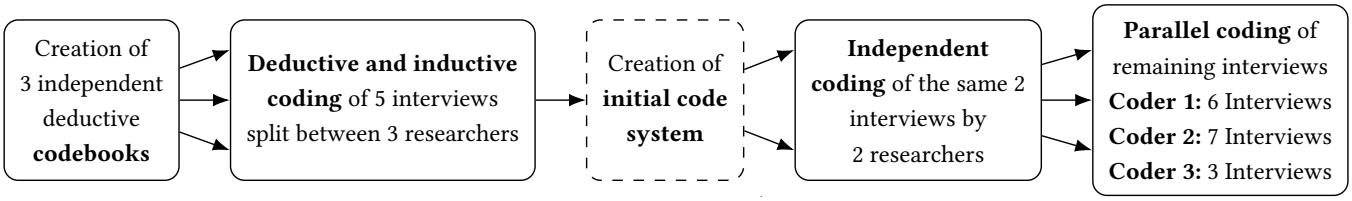

Figure 2: Process of the qualitative analysis conducted by three researchers

phone and social media (LinkedIn). The response rate was very low. We contacted 239 facilities, meaning individuals, hospitals or clinics (with the majority being individuals). Of the 239 facilities, 66 were from Germany, 17 were from England, and 156 were from America. In total, 20 facilities responded - 18 from Germany and two from America. Ultimately, only eight individuals participated in the study. The other 12 respondents did not express interest after the first contact. Every participant was offered a 40 Euro Amazon Voucher as compensation for their time. Two participants declined the voucher.

3.3 Analysis

We used Kuckartz et al. as as a guide for creating our codebook [37]. For the whole coding process we used the qualitative analysis software MAXQDA. Our analysis process is displayed in figure 2. Initially, three researchers each independently created a deductive preliminary codebook based on the interview guide. Subsequently, five interviews were split among the three researchers and each iteratively expanded their own codebook. Next, over multiple sessions, the three coders merged and summarized their distinct codebooks. The final codebook consisted of 16 codes and is illustrated in table 2. The categories *Procurement, Integration & Maintenance and Usage* were coded every time a coding from other categories clearly fell into one of the three phases. MAXQDA helped identify correlations among coded references, helping us to better understand coded statements in the context of the IoT life cycle and to support our further analysis. The first coder was assigned six interviews, the second one seven and the third one two interviews to code. We made sure during the assignment of the interviews that each interview was coded twice at the end. Two researchers started with coding the same two interviews, to check whether the code system worked, or if it required changes. As this worked well, we adopted the code system. Each researcher summarized longer coded references and developed individual memos to further enhance each individual coder's as well as the group's common understanding of the data. Finally we merged all coded references and summaries. Qualitative mythologists assert that the value of multiple coding iterations by different coders lies in the process rather than the product. Involving multiple coders is important to identify themes and disagreements contributing to the qualitative analysis of the data and to stimulate critical conversations, but focusing on statistics such as inter-rater reliability can actually be detrimental to the qualitative nature of the study. In accordance with this, the coding process was highly collaborative, but the inter-coder reliability was not calculated [8, 43].

3.4 Ethics & Data Protection

Our institution did not have an institutional review board (IRB) nor an ethics review board (ERB) for security research. We adhered to German and EU privacy laws and conducted the study after a consultation with a data protection officer of our institution. Our consent form is compliant with the European General Data Protection Regulation (GDPR) and covered all information usually needed for a US IRB approval. Participants were informed that participation was voluntary and that they could stop at any time and ask their data not to be used, without giving a reason. Within the consent form we also specified that we would only evaluate de-identified data and only publish aggregate data and de-identified quotes. For that reason, we abstracted some of the job descriptions reported by the participants. All participants consented to our data collection, data processing and publication strategy. At the beginning of each interview we deliberately resolved any remaining questions participants had. After transcribing the recorded interviews we destroyed the audio files.

4 RESULTS

In this section we first report the demographic data, and then present the key findings from the interviews in various categories: *Technical factors* 4.2, *organizational factors* 4.3, *manufacturers & security* 4.4 and *laws & regulations* 4.5.

4.1 Demographics

We interviewed eight participants, seven men and one woman, all from Germany, aged from 30 to 58 years. Their industry experience ranged from five to 32 years, with an average industry experience of 19,3 years. Our participants had a high level of education: Three participants had a vocational degree, three participants a master's/diploma and two participants a PhD. To protect our participants' identities we abstracted the reported job titles. Three interviewees were IT consultants, meaning they worked for hospitals; three interviewees were Internal IT, meaning they worked in hospitals; and two interviewees had worked in the hospital setting in the past.

Table 1: Demographic Data of our participants.

Gender	Male	7	Female	1
Age [years]	Min.	30	Max.	58
	Mean	46,4		
Industry Experience [years]	Min	5	Max	32
	Mean	19,3		
Education	Vocational Education	3	PhD	2
	Master / Diploma	3		

4.2 Technical Factors

4.2.1 Patch & Update Process. Most software updates are automatically and regularly deployed, but participants agreed that update and patch processes are more complicated for certified medical products. Participant 2, for instance reported that he set up a temporary VPN connection to allow the manufacturer to update the product - IT staff were not allowed to update the product because the server was also classified as a medical product and therefore the responsibility lies with the manufacturer. In this example a remote update was possible, but other participants reported having IoT systems that are updated manually - either by the manufacturers, who sends their own technicians, or by hospital-internal medical technicians. When participant 6 was asked who he thought was responsible for updating and patching medical systems, he answered that it varies: depending on the current service contracts, the organizational structure, and the size of the hospital, updates are deployed by a(n) *(intern) service technician*, *IT staff*, a *specialized department* or the *client service partner*. *"[...] I don't think you can give a general answer. Must be individually - There is [someone responsible for updating and patching] in each hospital but it can be organized differently in each hospital."* – [P6]. Participant 8 elaborated that the update and patch process may also be unable to take place in certain cases: *"In the hospitals in which it is probably hardly regulated, it [update/patch processes] also does not take place. Unless it results from some service technician's presence."* – [P6]. Participant 5 mentioned that - as devices become smaller, more needs to be done by the IT department: *"The smaller the devices become, the more this work is shifted to in-house IT. [...]"* – [P5]. Two participants noted challenges of software updates beyond IT security - they can interfere with device functionality: *"Yes, but one regularly experiences that a large company [...] installs software updates [...] and then interfaces do not work, where there is absolutely a causality to be seen, because it no longer works after the restart of the system, after the integration of the new software."* – [P3]. One participant reported that they set up a system to test updates in advance, to ensure they would not interrupt the system, because such interruptions can cause related processes to halt and be potentially life-threatening.

> The update process varies from device to device and is influenced by structural factors. In many cases the process happens manually and is a challenging procedure for the involved parties.

4.2.2 Outdated Systems. All participants reported that many medical systems are outdated, and that medical IT as a whole lags far behind technology used in other fields: *"Medical technology is often far behind, the devices have old software, still [MS] XP or so."* – [P1]. One participant even asserted that seeing [MS] Windows 10 on devices would *"be blatantly state of the art, if that would be supported by any manufacturer"* – [P7]. He further explained that older operating systems are still prevalent: *"So, of course, older operating systems will continue to be rolled out as the standard or state of the art, and you have to deal with that in the hospital."* – [P7]. Participant 3 described a related problem. They were supplied with devices containing [MS] Windows 10, but the manufacturer already announced that they would not provide future updates to a newer version. If the device's lifetime of 5-6 years is taken into account, this is troublesome from the participant's point of view: *"We know that [MS] Windows 10 is actually being phased out right now and that we have a half-life that is certainly still 5-6 years for the hardware. But [the manufacturer] has already announced that no more operating systems will be made available for this device."* – [P3]. He explained that it is not easy for a manufacturer to upgrade an operating system because this would require re-certification of the device - which is time-consuming and expensive: *"That's why manufacturers often go through this process for only one operating system version. Only if it is a device that has an extremely long service life, then perhaps another control unit with a more modern operating system is added."* – [P3]. One participant further elaborated that it is likely one will find old operating systems in nearly all hospitals, and that many of them think that there are no risks associated with older systems: *"It must still be assumed that there are certainly quite a few [devices with outdated operating systems] and many hospitals that have almost no networked medical technology at all and accordingly still assume that a Windows RT computer, which makes the image visualization on the ultrasound device, presents no risk at all"* – [P1].

> According to our participants, old systems are typical in hospitals and it can generally be assumed at the time of purchase that the lifetime of a medical device will exceed the duration of the software support. Devices are often in use for several operating system generations.

4.2.3 Compatibility. Seven participants mentioned interoperability problems - between older and newer devices, and between different manufacturers. Default protocols like the HL7[1] or DICOM[2] do exist, but the implementation and maintenance of device interfaces in practice poses challenges. The lifetime of some devices exceeds a decade and incompatibility problems with new devices, protocols, technologies and security standards arise: *"An ultrasound device has, I don't know, 5-6 years of service life, seven years of service life, an X-ray system has 15 to 25 years of service life, so that there are often technological leaps in the devices that are replaced.[...]"* – [P3]. The compatibility between different manufacturers in terms of installation and integration of IoT devices was frequently mentioned as a major problem. Market leaders develop their own interpretations of interfaces, which also impacts security: *"[...] I would say that each manufacturer is actually its own world and has its own security concepts, its own architecture, its own interfaces, and its own networking ideas.[...]"* – [P7]. Furthermore, the secure configuration of devices using the previously mentioned protocols seems to be rather unusable: *"The DICOM interfaces are really absolutely standardized. If you have three communication parameters and you configure them on the devices, maybe there are security settings that have to be set on the individual devices with this parameter."* – [P3].

> Standardised medical IoT protocols do not effectively prevent incompatibility of outdated interfaces and non-transparent solutions provided by different manufacturers, problems that ultimately pose a risk to security.

4.2.4 Primary Security Mitigation: Network Separation. All eight participants employed network separation to prevent security incidents involving medical IoT devices. Such separation works by (I) fully isolating IoT devices from the internet and (II) connecting

[1] https://www.hl7.org/, acccessed July 09. 2022
[2] https://www.dicomstandard.org/, accessed July 09. 2022

the IoT devices in an independent network, separate from the IT-network. This strict separation was primarily employed to ensure security and data privacy (in accordance with the GDPR): *"We have to make sure that we integrate it [the IoT device] into the network in such a way that a connection from the outside is as difficult as possible or even impossible"* – [P2]. The participants openly reported that separation is the primary mitigation strategy against attacks on outdated and vulnerable IoT devices and that there seems to be no practical alternative, even if this approach hinders usability: *"It's more likely that things are outdated and no longer meet security requirements, and the devices are then isolated in their own virtual LAN. In times of digitalization, this is bad, because then you have to print it [results from diagnostic measurements] and scan it. [...] You are just forced to – You either have to use analogue media or you are forced to buy a new product, to update data or to change to another manufacturer."* – [P1]. Network separation conflicts with the requirements of manufacturers who want to have a permanent connection to the devices to gather data and perform remote updates/maintenance: *"The manufacturers usually don't like this [the network separation], because of course they would like to have access to these devices even after they have been installed in the hospital. Many also require that the device send data to them as well – patient data. [...]"* – [P5].

It seems that manufacturers are winning the argument. One participant observed that the formerly strict stance on network separation has been softening, with hospitals allowing more and more remote access: *"Typically, hospitals rarely or never granted access to the network outside, or if they did, then only on request. However, the whole thing changed somewhat during my working time. [...]"* – [P2]. The participants also had thoughts on how to minimize attacks from within the hospital. They believe that the IoT devices are, to some degree, protected against direct access: *"[...] Such a system [IoT device] is not placed on the floor. Access to the devices is to some degree restricted and so you don't have big problems."* – [P3]. One participant also mentioned that even the usage of flash drives to transfer data from IoT devices is prohibited and blocked by devices: *"[...] no one comes to an MPG [person responsible for medical devices] with a USB stick that has not been released by us, plugs it in and downloads data or sends data to it.[...]"* – [P5].

> To mitigate the danger posed by outdated and vulnerable IoT devices, all eight participants reported that the separation of IoT devices into their own networks – without internet access – is common. The multitude of usability problems must yield to this mitigation strategy.

4.2.5 Unprotected Patient Data. The participants mentioned problems with the handling of patient data stored on and processed by IoT devices. Sometimes patient data is not correctly deleted, and is left accessible to other personnel that should not have access: *"The blood pressure monitor you plug in normally via USB, access the data carrier, get the data and if the doctor forgot to delete the data from the last patient, then you have everything."* – [P4]. In some cases an IoT device does not work until certain personal information is added: *"You can't get the blood pressure monitor to work if you don't transfer all the patient data to the blood pressure monitor beforehand, because the report is then generated from it [...]"* – [P4]. This adds to the reports that patient data is, in multiple cases, stored locally on the IoT devices: *"The person using the device must first identify the patient, e.g. get the data from the device to see which patient it is."* – [P5]. Participant experiences varied with regards to if IoT devices are, by any means, protected against direct unauthorized access (see also section 4.3.3): Participant 1, for example, reported that logins are not always required: *"There are devices, such as sonographic devices, that you turn on and there is no user login."* – [P1]. Participant 3 reported the same, adding that patient data is accessible without authentication: *"So you don't usually have to log in to a sonographic device to take actions there, to retrieve patient lists."* – [P3]. On other devices, however, a login is required: *"Blood glucose monitors, you have to log in with a username, person-related. Then there are devices, historically older devices, which are password protected but there is just a password for everyone."* – [P1].

> Sometimes sensitive patient data is stored on medical IoT devices without protection against unauthorized access.

4.3 Organizational Factors

4.3.1 Responsibility. Participants mentioned many stakeholders in the hospital environment responsible for IoT security: medical departments, medical technicians, IT, manufacturers, management, a cyber defense center (from an external provider), users, law makers & regulators. Participants did not have a unified opinion as to who is responsible for IoT Security. Four participants argued that the management is responsible: *"Look at the very top, it's him or her. He or she bears the responsibility, can't delegate it, can only delegate the tasks, and in the end has to bear the responsibility and take the rap, and many people don't realize that."* – [P4]. One participant reported that everyone is responsible in some form or another: *"All of them. There are areas that have this on their business card or in their signature, but security is something that everyone has to implement and shape, just like data protection, just like hygiene in a hospital. [...]"* – [P7]. Five participants mentioned that the responsibility is often passed between stakeholders: *"The problem I see here is that current security concepts are usually broken down to the last and weakest link, in the example we just had 'The nurse who wants to do her job'. "* – [P2]. One participant even stated that everyone has the responsibility, but excluded himself in the very next sentence: *"Everyone is responsible for security. The more you know about it, the more responsible you are, I would say. My current role is basically just integration. In this respect, I am hardly responsible for security at all."* – [P2]. Two participants also reported security problems caused by the fear of taking responsibility, with the manufacturer of IoT devices as an example: *"The whole thing then also leads to many manufacturers saying: "No, we'd rather use Windows, then at least we know who is to blame". Which doesn't mean that we have a higher security in the end, maybe even a higher vulnerability [...] "* – [P2]. The distribution of responsibility also differed based on the size and sophistication of the organization. One organization, for example, had a dedicated cyber defense center: *"[...] and we have a cyber defense center. A cyber defense center that is responsible for all our hospitals, [...] "* – [P1].

> It is not clear who is responsible for the security of IoT devices in hospitals. The responsibility varies based on the size and sophistication of the organization. Oftentimes, a "diffusion of responsibility" occures.

4.3.2 Resources. Six participants explicitly mentioned that they either do not have the resources for security or that they have experienced cases where a hospital did not have enough resources

for IT security: *"Resources or personnel resources is basically a problem in hospitals. There are certainly exceptions to this, if you take large university hospitals [...] "* – [P5]. One participant even witnessed hospitals in which *"In some cases, I have seen IT departments assigned to janitors."* – [P2]. Contrarily, one participant, who works in a larger hospital, mentioned that resources are sufficient for security at his employer. The hospital he works for has a dedicated security operation center: *" [...] Yes, we will definitely get enough resources. Even now with the KHZG, Hospital Future Act. You get subsidies, something is already coming, yes. I think people have recognized that. Late, but it was recognized."* – [P1]. Participant 3 added: *"In the past resources for IT was clearly an economic problem. Because the upgrading on the hospital side with necessary protection mechanisms was simply not financed, only a few hospitals had an understanding of this."* – [P3]. The same participant compared an IT department in business to an IT department in hospitals: *"You will quickly find that an IT employee is responsible for 20, 30 users or so. In a hospital environment, an IT employee is responsible for 100 to 150 users,[...] "* – [P4]. When participant 7 was asked whether he received enough resources at his former employer (10 years ago) for security, he laughed and explained that this is still a problem today: *"No [Laughs] [...] Of course, this is also an important point that has not yet been implemented in such an ideal way."* – [P7].

> The technical staff in hospitals is rather sparse and has to take care of a large number of different systems. Larger hospitals seem to be better equipped, although this may vary from case to case.

4.3.3 User Security Behaviour & Attitudes. In German hospitals, a shortage of medical staff (doctors, nurses and others) leads to most feeling they have insufficient time to discharge their primary task - patient care. Thus, it is not surprising that time-consuming security tasks will be bypassed [36]. Our participants report that the security mechanisms for most IoT devices are circumvented because they are not usable, so medical staff's compliance budget is exhausted quickly *compliance budget* [9]. The most mentioned examples are shared accounts and passwords written down on devices: *"Passwords, shared passwords, passwords that are written under the keyboard, passwords that are passed on, computers that are not locked [...]."* – [P6]. Participant 1 explicitly noted that auto log out procedures directly oppose the primary task of medical staff, but still criticized the (necessary) circumvention: *"In the hospitals every day stress, people have little time [...] people document with someone else's account, someone has locked their password and doesn't have time to call IT and just use a colleague's account. That's commonplace, unfortunately."* – [P1]. Security measures designed for IT environments do not necessarily work in a hospital, e.g. because medical personnel needs to wear medical gloves: *"Classic methods with RFID cards, fingerprints and the like... These are things that you would classify as usable, but which also have a high level of security. However, such procedures are often not available in the environments because they have areas where they work with gloves."* – [P3]. Participant 4 holds the security personnel accountable for unusable security and bad password policies: *"Security measures cost extra time, cost extra care, I have to take a special step. Sometimes the security measures are not even feasible. These are very bad security measures, because they erode the entire system. But IT security people are not afraid to demand security measures that are simply banal and far too complicated. The famous example is password policies. Everywhere on every [IoT] device I need a password with upper and lower case letters, numbers, special characters, at least 10 digits."* – [P4].

> The time pressure on medical staff leads to the circumvention of security rules, e.g. in the form of account sharing, password memos on devices and log out prevention. The participants partially express an understanding for this behaviour, but blame the medical staff or the security personal for such practices.

4.3.4 Security Incidents. When asked about specific security incidents that had occurred, five participants reported that either no security incidents had occurred or that they were not significant: *"So as I said, no direct real critical incident that I know of. Everything has been smooth so far. "* – [P3]. Two participants noted that it was by sheer luck serious incidents had not happened: *"[...]All that protected them from a possible attack is once the fact that probably no motivated attacker was there. Luck.[...] "* – [P2]. When asked about the likelihood of security incidents in the future, six participants reported that it was very likely: *"I think that is very high, probably. "* – [P8]. One participant described incidents that had taken place in other organizations. Two participants noted that external security incidents helped create a sense of urgency and awareness in their internal management: *" Recently, we have had a relatively large number of discussions with management, where it is very important because they have seen it in the environment. Especially these ransomware attacks, which we see massively in the economy but also in the hospital environment [...]. Yes, it is leading many people to think about it now. People are not stupid. They haven't had this on their radar yet [...]"* – [P4].

> Security incidents with IoT devices either have not occurred within the organizations of the participants or were not notable. Still, participants asserted that incidents have been avoided by luck and are very likely to arise in the future.

4.4 Manufacturers & Security

Participant 1 mentioned the Log4J vulnerability [52], and explained that only one or two manufacturers reported independently on this. This was the only time the participant felt supported in terms of security by the manufacturer: *"So actively supported not, no. I don't know now, except for the one thing where a manufacturer once wrote to me about a security gap: "You have the Log4J gap" [...]. "* – [P2]. He also explained that the security department had to scan all devices in the network and report the findings to the manufacturers. Participant 4 also expressed that the IT department typically initiated conversations with the manufacturer: *"[...] It is often the other way around, that an internal test somehow reveals that the big device still runs on a completely old operating system, and then you get into arguments with the manufacturers. "* – [P4]. Some manufacturers lag behind the state-of-the-art and sell outdated systems: *"An example of this is when a system is shipped with Windows XP. However, if the manufacturer has certified that the system is harmless, the managing director has often told the data protection officer in the last instance: "If [the manufacturer] says so, then there are no concerns. "* – [P3]. The same participant also explained that they ask manufacturers to provide information the IT department needs to manage the device effectively, but rarely receive all requested information: *" The larger and more well-known the group is, the less they get this table back.*

Even on request, partly only rudimentary filled out. " — [P3]. Participant 5 explained that they try to test new systems before integration, but that they are limited by the manufacturers: *"Apart from the fact that in most cases we can't look into the programming in detail, we can only ask the usual questions and get a description of what specific software on the server does."* — [P5]. Three participants mentioned that manufacturers are interested in receiving and processing patient data. Furthermore, the usage of cloud services was described as challenging in the past: *"That was still a very difficult topic, because many medical technology device manufacturers also offer these cloud services for corresponding evaluations, for corresponding benchmarking, for error analyses. This has not been possible until now."* — [P7].

It is often difficult to obtain all necessary technical information from manufacturers and much remains ambiguous, especially with regard to security. Additionally, manufacturers have a heightened interest in obtaining and processing patient data.

4.5 Laws & Regulations

Generally, the laws regarding IT security in healthcare were described as having a positive impact. First, regulations put pressure on the organizations themselves, as participant 5 said: *"Due to the IT Security Act 2.0 and the KHZG, they are now forced to think more intensively about this [IT security] and that is also the reason why everyone, most hospitals at least, are now looking for people who can work in this area. [...] "* — [P5]. Second, regulations put pressure on the manufacturers, as participant 6 described: *"In the case of medical devices, we have the Medicine Device Regulation, which of course also requires corresponding safety and security queries. Within the framework of the MDR and the BSI, there are corresponding questionnaires, safety questionnaires, which the manufacturers should observe and which, I say, must be available as a minimum standard."* — [P6]. Two participants mentioned the KRITIS regulation and its positive impact it has on security: *"[...] For the first time, a much higher level of awareness has emerged. On all sides. Because the hospitals now also have a possibility to demand this safety and can now also exert a certain market pressure, because we can now say: "You do not fulfill legal requirements and therefore your product is no longer included in the selection"[...]."* — [P3]. Three participants also said that employees who operate such devices now have to undergo mandatory trainings. As participant 1 described: *"[...] there is, for example, in the Medical Devices Ordinance that every employee who uses such a product must be trained, for example.[...]"* — [P1]. Contracts with the manufacturer were described by three participants as an important part of the relationship, to guarantee the technical support of the devices. Participant 5 noted: *"Most hospitals go for this maintenance contract anyway and always, because then you have the possibility to get or secure the support of the manufacturer directly if any errors occur."* — [P5]. Even though legal constraints were seen to be positive overall, the certification of IoT devices was seen as a constraint for security by four participants: *"[...][the manufacturers] say: "Well, we are not allowed to change anything, because the moment we change a component and that would also be, for example, an operating system update, we would have to re-certify. We would lose our certification and that is not possible at this point"."* — [P6].

Participants generally had a positive view of the laws and regulations regarding security in healthcare, noting the pressure that it puts on organizations and manufacturers. However, the certification process of IoT devices can hinder the mitigation of security issues

5 DISCUSSION

In this section, we discuss our findings and provide recommendations for industry and academia.

5.1 Factors Impacting Security

In response to our research question, we have identified various factors that influence the security of medical IoT devices, which often impact other aspects of security in hospitals.

Missing Security Transparency. Manufacturers frequently fail to provide sufficient information about what data is transmitted and how the technology works. Even when contacting manufacturers, many inquiries remain unanswered and the procurement proceeds. Therefore, hospital IT staff have to trust manufacturer statements since they cannot check what exactly is being transmitted. That leads some IT staff to seal devices off as best as they can (see 4.2.4 and 5.3) - a problem that has also been identified by IoT research in other sectors [16]. Even within the hospital many processes are unclear because the responsibility for maintenance and integration is divided between different departments (*IT, medical technicians, security*) and they do not always collaborate (see 4.3.1).

Long, diverse & chaotic maintenance processes. We noticed substantial difference in processes around medical IoT devices. Responsibility for updates was assigned to IT, medical technology or even the manufacturer, depending on the device, staffing levels and staff expertise. There is no central register that keeps track of which devices need to be updated, and when. One participant even reported that updates are carried out almost weekly (mostly deployed locally by medical technicians or the manufacturer), and IT usually only notices the consequences (see 4.2.1). The lack of a standard process for a single security task (updating) means there is a high potential for error, and/or the job not being done at all. If updates are carried out by the manufacturer or service partners, the competence should be higher, but it tends to delay the task being done. This can then lead to systems being outdated (see 4.2.2 and 5.1). In the example of the log4J vulnerability [52], where thousands of devices deployed in hospitals were affected, only one participant mentioned the hospital being actively approached by the manufacturer about it. The IT department, on the other hand, found many more systems vulnerable to log4J and needed to actively contact the manufacturers for feedback. Furthermore, the replacement of defective devices also involves an increased risk, as patient data may still remain on the devices, and network interfaces must also be adapted accordingly. Devices may be send back to the manufacturer, service partner or resold elsewhere.

Outdated Systems. Outdated operating systems (e.g. systems running still Windows XP) and unpatched IoT devices are common and were reported by all participants. There are a multitude of reasons for this: (I) The End-of-life > End-of-Service for devices used for more than a decade. (II) Updates are often not provided by the manufacturers, since some updates require a full re-certification of the device, following the MP act [17]. That process is lengthy

and the MP act does not seem to accommodate modern software requirements. (III) If updates are provided, they cannot easily be applied due to the mitigation strategy for most medical IoT devices (see also 5.3). Additionally the update strategy and the responsible party varies by device, often prolonging time until the update can be completely deployed.

Limited Resources. IT departments in hospitals are understaffed more often than not, which leaves a small number of individuals to maintain a multitude of applications and networks. Small hospitals and practices struggle to a larger degree due to more limited funds. We even heard of a case where the janitor was, at the same time, to carry out the duties of the IT department. This, of course, has a significant impact on security, as many participants reported that manufacturers' support often stops at the network jack on the wall, and the IT department is responsible for everything after. We also heard that servers for medical IoT devices must sometimes be deployed by the IT staff. Cloud technologies, as typically known from the IoT environment, also exist in the medical sector, but the participants expressed criticism here with regard to security and data protection. Lack of competence and understaffing of IT personnel may lead to security and privacy problems.

(Usable) Security Awareness. Functionality and safety of medical IoT devices is (understandably) more important to manufacturers, medical technicians and hospital management than IT security [16]. It is only since a change in the MP act in 2020 that the stakeholder really consider the topic of IT security. So far it is unclear what practical implications this greater awareness has. When it comes to the medical staff we are unable to make a statement about their security awareness based on our data: Yes, the staff circumvent security, but only to fulfill their duties. We cannot say whether they are aware of the risks posed by their behaviour.

5.2 Major Incident Reports

While most participants reported some security and privacy incidents (like unsecured patient data not deleted from devices and local infections via flash drives), none of them reported a major incident that occurred during their career involving medical IoT devices. One explanation for this could be that medical IoT devices in hospitals are not a worthwhile target,[3] or that the security strategy of isolating IoT devices from the internet is effective against remote attackers. As the Russian war against Ukraine in 2022 showed, the first explanation may be plausible in times of peace, but hospitals and their medical IoT devices are vulnerable targets in times of war.[4] As always, there is also the possibility that participants did not want to admit that major incidents happened.

5.3 Consequences & Risks of Current Mitigation Strategies

All participants reported that the full isolation of IoT devices from the internet and/or separation in own network segments is the most common mitigation strategy. Such isolation has a negative impact on the usability: (I) Automated updates are not possible without further effort. (II) The manufacturers cannot perform remote debugging and maintenance. (III) Medical staff and patients shift from digital to fully analogue processes to exchange data between devices, services and departments. Furthermore, the root cause of security problems (outdated devices, devices' nontransparent security behaviour) is not tackled. Rather, a curtain is drawn to cover and shield access to those vulnerabilities. This mitigation fully ignores internal threats and no participant reported any form of in-depth defence strategy – so, one exploited vulnerability could have fatal consequences and could persist undetected due to the use of network covert channels [60] that also cross typical network separation and isolation boundaries. Internal threats are a known problem when it comes to the forbidden access of sensitive data by unauthorized personnel, e.g. in the police.[5] This could very well also be a problem in hospitals where sensitive patient data stored on IoT devices is accessible to most medical personnel. Patients are also commonly left alone in treatment rooms with direct access to the IoT devices. Interestingly, some participants reported that they make regular exceptions to the isolation strategy and open the network for single data transfers or patches, undermining the mitigation strategy. The mitigation strategy of blocking external communication may work, but as manufacturers increasingly desire to attain more patient data (see 5.1) to improve their services, a new need for connecting devices to the internet arises. We expect that more medical devices will be connected to a centralized system located at manufacturers, as this is currently observed in other industries [28].

5.4 Implications for Industry and Authorities

Security Transparency. Participants reported many cases where manufacturers kept their security architecture a secret. This creates mistrust among the IT staff and we conclude that this is one major reason IT departments are compelled to isolate devices from the internet. In terms of security, this strategy *Security-by-Obscurity* is not recommended and violates the second Kerckhoff's principle [33]. We see trends moving towards security and privacy in hospitals, and therefore advise manufacturers to work specifically on improving the transparency with regards to data handling and security. This does not necessarily have to be the publication of code – a security white paper could be a good start. Previously, Sametinger et al. [53], found problems with the transparency of the security processes of medical devices. Morgner et al. [47], proposed that updates for (private) IoT devices should be secured with transparent labels – a technique that could also help here.

Make use of privacy technologies. While privacy laws differ in countries outside the EU, manufacturers and their products still need to be compliant with the GDPR when using patient data. As manufacturers may be interested in processing data from many hospitals, concepts like differential privacy [20] could be used in specific cases to prevent backtracking of patient identities, even if a data leak occurs. Also, manufacturers should communicate transparently how their products' features contribute towards GDRP

[3] In 2020 a ransomware gang even handed out the decryption key to the university hospital in Düsseldorf [44], after they realized that they did attack a hospital rather than an university.

[4] https://www.who.int/news/item/07-04-2022-who-records-100th-attack-on-health-care-in-ukraine, accessed June 10. 2022

[5] https://www.computerworld.com/article/3124641/cops-run-unauthorized-searches-on-confidential-databases-for-revenge-stalking.html, accessed June 10. 2022

compliance, as our participants reported that this is most often required and enforced during the procurement process. Privacy communication should also be transparent. The IT department and other stakeholders should easily be able to judge whether and how specific solutions fulfill the GDPR.

Regulations and government programs have impact. We also noticed that our participants, some of whom have several decades of industry experience in the medical sector, mentioned that they have noticed security improving recently. This may come from changes in the MP act 2020 [17] and the classification of hospitals as critical infrastructures. The issue of privacy and the way hospitals and manufacturers deal with it has also improved with the GDPR.

Support the IT departments. The IT staff in hospitals usually maintains two networks, where the network including medical devices contains a variety of different devices, each with different standards. This challenges the largely understaffed IT personnel. The IT departments of hospitals and smaller medical facilities need more support. Smaller facilities are currently performing worse than larger facilities in terms of security based on statements of our participants.

5.5 Implications for Academia

Our sample may apply mostly to the German healthcare system. While this shares similarities with other EU country's systems, it may differ in some regards. Processes and systems may significantly differ from those in the US and non-EU countries. In the EU, for example, GDPR impacts the procurement and use of medical IoT devices. We strongly recommend extending our research, as the problems and challenges related to medical IoT devices should be investigated holistically. Therefore we recommend (I) Replicating this study with IT healthcare professionals from other countries, especially outside of the EU. As participants may only explain things from their point of view, we also strongly recommend to (II) investigate the perspective of the manufacturers and regulatory authorities. Additionally, security must also be usable, as otherwise the best technical security measure may be misused, bypassed or simply not adopted by users. Users should not be blamed, as the origin of this problem lies in the provided technology. Therefore, software should be designed to avoid such problems from the start and research with the development teams of the manufacturers, which so far struggle with this task, should be performed [26]. Moreover, we suggest to also (III) investigate the actual users of medical IoT devices, to derive comprehensive advice for the manufacturers and IT departments.

5.5.1 In-depths case investigation. Not all strategies and processes currently in place are bad. Our participants also described cases in which security was handled well and where it was part of most processes. Investigating security cultures and processes of well-performing hospitals in detail may allow abstracting and transferring best practices. This could help improve security practices and processes of less sophisticated facilities. In addition, those finding would also support regulation authorities and government institutions when deriving and enforcing good practices, new regulations and support packages for the healthcare industry.

5.6 Limitations

There are several limitations within this work. We captured only a small sample of German IT professionals from the healthcare sector. Hence, our findings may not cover all factors and trends impacting security and may differ in other regions. Nevertheless, our participants worked on both domestic and international projects and had an average industry experience of almost 20 years. Participants may have also failed to mention important aspects and may be biased by their past experiences, potentially biasing our results. As this is a qualitative study, our results should not be generalized and may not be applicable to the whole population. The healthcare sector encompasses a wide range of regulatory requirements, measures and processes. Since most interviews were conducted in German, the quotes we present are translated. We have taken great care with the translation, but cannot guarantee that individual contexts fit.

6 CONCLUSION

In this study, we investigated challenges associated with the securing of medical IoT in a hospital context. We interviewed eight security specialists with significant experience in this context. We discovered a diverse set of interconnected factors that impact the security of IoT-devices in hospitals, from technical aspects (i.e. outdated systems) to organizational aspects (i.e. limited resources and the delegation of responsibility). We also discovered that laws and regulations improved security of hospitals over the last years and that the relationship between medical device manufacturers needs to be improved: lack of trust and transparency is not a basis for the "collective defence" approach. A clear definition of individual and joint responsibilities is a first step, but there also needs to be a commitment to not hide problems from each other, and a process of evaluating and improving security.

ACKNOWLEDGMENTS

We want to thank all participants of our study and the anonymous reviewers for their helpful feedback. The research was primarily funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - EXC 2092 CASA - 390781972 and also (partly) by the PhD School "SecHuman - Security for Humans in Cyberspace" by the federal state of NRW, Germany.

REFERENCES

[1] Nasser S Abouzakhar, Andrew Jones, and Olga Angelopoulou. 2017. Internet of things security: A review of risks and threats to healthcare sector. In *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. IEEE, Exeter, UK, 373–378.

[2] Nur Azaliah Abu Bakar, Wan Makhtariah Wan Ramli, and Noor Hafizah Hassan. 2019. The internet of things in healthcare: an overview, challenges and model plan for security risks management process. *Indonesian Journal of Electrical Engineering and Computer Science* 15, 1 (2019), 414.

[3] Farhad Ahamed and Farnaz Farid. 2018. Applying internet of things and machine-learning for personalized healthcare: Issues and challenges. In *2018 International Conference on Machine Learning and Data Engineering (iCMLDE)*. IEEE, Sydney, NSW, Australia, 19–21.

[4] Muhammad Mahtab Alam, Hassan Malik, Muhidul Islam Khan, Tamas Pardy, Alar Kuusik, and Yannick Le Moullec. 2018. A survey on the roles of communication technologies in IoT-based personalized healthcare applications. *IEEE Access* 6 (2018), 36611–36631.

[5] Suvini P Amaraweera and Malka N Halgamuge. 2019. Internet of things in the healthcare sector: overview of security and privacy issues. *Security, privacy and trust in the IoT environment* 1 (2019), 153–179.
[6] Danielle GT Arts, Nicolette F De Keizer, and Gert-Jan Scheffer. 2002. Defining and improving data quality in medical registries: a literature review, case study, and generic framework. *Journal of the American Medical Informatics Association* 9, 6 (2002), 600–611.
[7] Maria Bada, Angela M Sasse, and Jason RC Nurse. 2019. Cyber security awareness campaigns: Why do they fail to change behaviour?
[8] Rosaline S Barbour. 2001. Checklists for improving rigour in qualitative research: a case of the tail wagging the dog? *Bmj* 322, 7294 (2001), 1115–1117.
[9] Adam Beautement, M. Angela Sasse, and Mike Wonham. 2008. The compliance budget: Managing security behaviour in organisations. In *Proceedings of the 2008 Workshop on New Security Paradigms*, Angelos Keromytis, Anil Somayaji, Christian W. Probst, and Matt Bishop (Eds.). Association for Computing Machinery, New York, 47.
[10] Bundesnetzagentur. 2017. *Bundesnetzagentur zieht Kinderpuppe „Cayla" aus dem Verkehr.* Bundesnetzagentur. https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2017/14012017_cayla.html
[11] Carmen Camara, Pedro Peris-Lopez, and Juan E Tapiador. 2015. Security and privacy issues in implantable medical devices: A comprehensive survey. *Journal of biomedical informatics* 55 (2015), 272–289.
[12] Felipe Caro and Ramin Sadr. 2019. The Internet of Things (IoT) in retail: Bridging supply and demand. *Business Horizons* 62, 1 (2019), 47–54.
[13] National Cyber Security Centre. 2021. *Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board Annual Report 2021.* National Cyber Security Centre. https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-hcsec-oversight-board-annual-report-2021
[14] Lorrie Faith Cranor and Simson Garfinkel. 2004. Guest Editors' Introduction: Secure or Usable? *IEEE security & privacy* 2, 5 (2004), 16–18.
[15] KR Darshan and KR Anandakumar. 2015. A comprehensive review on usage of Internet of Things (IoT) in healthcare system. In *2015 International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT).* IEEE, Mandya, India, 132–136.
[16] Roberta De Michele and Marco Furini. 2019. Iot healthcare: Benefits, issues and challenges. In *Proceedings of the 5th EAI International Conference on smart objects and technologies for social good.* ACM, New York, NY, USA, 160–164.
[17] Deutscher Bundestag. 2020. Gesetz über Medizinprodukte (German): MPG.
[18] Deutscher Bundestag. 2021. Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz: BSI-KritisV (German).
[19] Deutscher Bundestag. 2022. Gesetz für ein Zukunftsprogramm Krankenhäuser: KHZG (German).
[20] Cynthia Dwork. 2006. Differential Privacy. In *Automata, Languages and Programming*, Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 1–12.
[21] Bahar Farahani, Farshad Firouzi, Victor Chang, Mustafa Badaroglu, Nicholas Constant, and Kunal Mankodiya. 2018. Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. *Future Generation Computer Systems* 78 (2018), 659–676.
[22] Muhammad Shoaib Farooq, Shamyla Riaz, Adnan Abid, Tariq Umer, and Yousaf Bin Zikria. 2020. Role of IoT technology in agriculture: A systematic literature review. *Electronics* 9, 2 (2020), 319.
[23] Jim Finkle. 2016. J&J warns diabetic patients: Insulin pump vulnerable to hacking. *Reuters. Published October* 4 (2016), 1.
[24] Farshad Firouzi, Bahar Farahani, Mohamed Ibrahim, and Krishnendu Chakrabarty. 2018. Keynote Paper: From EDA to IoT eHealth: Promises, Challenges, and Solutions. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 37, 12 (2018), 2965–2978.
[25] Ivan Flechais, M Angela Sasse, and Stephen MV Hailes. 2003. Bringing security home: a process for developing secure and usable systems. In *Proceedings of the 2003 workshop on New security paradigms.* ACM, New York, NY, USA, 49–57.
[26] Marco Gutfleisch, Jan H Klemmer, Niklas Busch, Yasemin Acar, M Angela Sasse, and Sascha Fahl. 2022. How does usable security (not) end up in software products? results from a qualitative interview study. In *43rd IEEE Symposium on Security and Privacy, IEEE S&P.* IEEE, San Francisco, CA, USA, 22–26.
[27] Xiali Hei, Xiaojiang Du, Shan Lin, Insup Lee, and Oleg Sokolsky. 2014. Patient infusion pattern based access control schemes for wireless insulin pump system. *IEEE Transactions on Parallel and Distributed Systems* 26, 11 (2014), 3108–3121.
[28] Sebastian Hermes, Tobias Riasanow, Eric K. Clemons, Markus Böhm, and Helmut Krcmar. 2020. The digital transformation of the healthcare industry: exploring the rise of emerging platform ecosystems and their influence on the role of patients. *Business Research* 13, 3 (2020), 1033–1069.
[29] Chi Yan Hui, Brian McKinstry, Olivia Fulton, Mark Buchner, and Hilary Pinnock. 2021. Patients' and Clinicians' Perceived Trust in Internet-of-Things Systems to Support Asthma Self-management: Qualitative Interview Study. *JMIR mHealth and uHealth* 9, 7 (2021), e24127.
[30] SM Riazul Islam, Daehan Kwak, MD Humaun Kabir, Mahmud Hossain, and Kyung-Sup Kwak. 2015. The internet of things for health care: a comprehensive survey. *IEEE access* 3 (2015), 678–708.
[31] Fariha Tasmin Jaigirdar, Carsten Rudolph, and Chris Bain. 2019. Can I trust the data I see? A Physician's concern on medical data in IoT health architectures. In *Proceedings of the Australasian computer science week multiconference.* ACM, New York, NY, USA, 1–10.
[32] Gulraiz J Joyia, Rao M Liaqat, Aftab Farooq, and Saad Rehman. 2017. Internet of medical things (IoMT): Applications, benefits and future challenges in healthcare domain. *J. Commun.* 12, 4 (2017), 240–247.
[33] Auguste Kerckhoffs. 1883. *La cryptographie militaire, ou, Des chiffres usités en temps de guerre: avec un nouveau procédé de déchiffrement applicable aux systèmes à double clef.* Librairie militaire de L. Baudoin, London, UK.
[34] Sung-Ho Kim and Kyungyong Chung. 2015. Emergency situation monitoring service using context motion tracking of chronic disease patients. *Cluster Computing* 18, 2 (2015), 747–759.
[35] Iacovos Kirlappos and M Angela Sasse. 2014. What usable security really means: Trusting and engaging users. In *International Conference on Human Aspects of Information Security, Privacy, and Trust.* Springer, ACM, New York, NY, USA, 69–78.
[36] Ross Koppel, Sean Smith, Jim Blythe, and Vijay Kothari. 2015. Workarounds to computer access in healthcare organizations: you want my password or a dead patient? In *Driving Quality in Informatics: Fulfilling the Promise.* IOS Press, Dartmouth, PA, USA, 215–220.
[37] Udo Kuckartz. 2012. *Qualitative inhaltsanalyse.* Beltz Juventa, Weinheim, Germany.
[38] Priyan Malarvizhi Kumar, S Lokesh, R Varatharajan, Gokulnath Chandra Babu, and P Parthasarathy. 2018. Cloud and IoT based disease prediction and diagnosis system for healthcare using Fuzzy neural classifier. *Future Generation Computer Systems* 86 (2018), 527–534.
[39] Alexandra R Lang, Jennifer L Martin, Sarah Sharples, and John A Crowe. 2013. The effect of design on the usability and real world effectiveness of medical devices: a case study with adolescent users. *Applied ergonomics* 44, 5 (2013), 799–810.
[40] Áine MacDermott, Phillip Kendrick, Ibrahim Idowu, Mal Ashall, and Qi Shi. 2019. Securing things in the healthcare internet of things. In *2019 Global IoT Summit (GIoTS).* IEEE, Aarhus, Denmark, 1–6.
[41] Taha Mansouri, Mohammad Reza Sadeghi Moghadam, Fatemeh Monshizadeh, and Ahad Zareravasan. 2021. IoT data quality issues and potential solutions: a literature review.
[42] Argyro Mavrogiorgou, Athanasios Kiourtis, Konstantinos Perakis, Stamatios Pitsios, and Dimosthenis Kyriazis. 2019. IoT in healthcare: Achieving interoperability of high-quality data acquired by IoT medical devices. *Sensors* 19, 9 (2019), 1978.
[43] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–23.
[44] Tom McVey. 2022. Ransomware recap: Learning from 2021.
[45] Francesca Meneghello, Matteo Calore, Daniel Zucchetto, Michele Polese, and Andrea Zanella. 2019. IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices. *IEEE Internet of Things Journal* 6, 5 (2019), 8182–8201.
[46] Emna Mezghani, Ernesto Exposito, Khalil Drira, Marcos Da Silveira, and Cédric Pruski. 2015. A semantic big data platform for integrating heterogeneous wearable data in healthcare. *Journal of medical systems* 39, 12 (2015), 1–8.
[47] Philipp Morgner, Christoph Mai, Nicole Koschate-Fischer, Felix Freiling, and Zinaida Benenson. 2020. Security Update Labels: Establishing Economic Incentives for Security Patching of IoT Consumer Products. In *2020 IEEE Symposium on Security and Privacy (SP).* IEEE, San Francisco, CA, USA, 429–446.
[48] Farha Nausheen and Sayyada Hajera Begum. 2018. Healthcare IoT: benefits, vulnerabilities and solutions. In *2018 2nd International Conference on Inventive Systems and Control (ICISC).* IEEE, Coimbatore, India, 517–522.
[49] Rahul Krishnan Pathinarupothi, P Durga, and Ekanath Srihari Rangan. 2018. IoT-based smart edge for global health: Remote monitoring with severity detection and alerts transmission. *IEEE Internet of Things Journal* 6, 2 (2018), 2449–2462.
[50] Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2019. Why people (don't) use password managers effectively. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019).* USENIX Association, Santa Clara, CA, USA, 319–338.
[51] Karen Rose, Scott Eldridge, and Lyman Chapin. 2015. The internet of things: An overview. *The internet society (ISOC)* 80 (2015), 1–50.
[52] Alexander Rudolph. 2022. What is Log4j and Why Did the Government of Canada Turn Everything Off?
[53] Johannes Sametinger, Jerzy Rozenblit, Roman Lysecky, and Peter Ott. 2015. Security challenges for medical devices. *Communications of the ACM* 58, 4 (2015), 74–82.
[54] M Angela Sasse and Ivan Flechais. 2005. Usable security: Why do we need it? How do we get it? In *Security and Usability: Designing secure systems that people can use.* O'Reilly, Sebastopol,CA, US.

[55] M. Angela Sasse, Jonas Hielscher, and Marco Gutfleisch. 2022. Human-Centred Security: Unfug Informationssicherheits-Sensibilisierung (German). *kma - Klinik Management aktuell* 27, 04 (2022), 44–46.
[56] Sureshkumar Selvaraj and Suresh Sundaravaradhan. 2020. Challenges and opportunities in IoT healthcare systems: a systematic review. *SN Applied Sciences* 2, 1 (2020), 139.
[57] Noman Shahid and Sandhya Aneja. 2017. Internet of Things: Vision, application areas and research challenges. In *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*. IEEE, Palladam, India, 583–587.
[58] Diane M Strong, Yang W Lee, and Richard Y Wang. 1997. Data quality in context. *Commun. ACM* 40, 5 (1997), 103–110.
[59] Dina Truxius, Müller Emanuel, Nikolai Krupp, Julian Suleder, Oliver Matula, and Dennis Kniel. 2020. BSI-Projekt 392: Manipulation von Medizinprodukten (ManiMed): Cyber-Sicherheitsbetrachtung vernetzter Medizinprodukte.
[60] Steffen Wendzel, Luca Caviglione, Wojciech Mazurczyk, Aleksandra Mileva, Jana Dittmann, Christian Krätzer, Kevin Lamshöft, Claus Vielhauer, Laura Hartmann, Jörg Keller, and Tom Neubert. 2021. A Revised Taxonomy of Steganography Embedding Patterns. In *The 16th International Conference on Availability, Reliability and Security*. ACM, New York, NY, USA, 1–12.
[61] Ka-Ping Yee. 2004. Aligning security and usability. *IEEE Security & Privacy* 2, 5 (2004), 48–55.
[62] Fotios Zantalis, Grigorios Koulouras, Sotiris Karabetsos, and Dionisis Kandris. 2019. A review of machine learning and IoT in smart transportation. *Future Internet* 11, 4 (2019), 94.
[63] Guanglou Zheng, Guanghe Zhang, Wencheng Yang, Craig Valli, Rajan Shankaran, and Mehmet A Orgun. 2017. From WannaCry to WannaDie: Security trade-offs and design for implantable medical devices. In *2017 17th International Symposium on Communications and Information Technologies (ISCIT)*. IEEE, Cairns, QLD, Australia, 1–5.

A PRE-QUESTIONNAIRE

Q1.1. How old are you?

Q1.2. What is your gender?

- Options: Male, Female, Non-binary / third gender, Prefer not to say, Prefer to self-describe

Q1.3. What is the highest level of school you have completed or the highest degree you have received?

- Options: Less than high school / GCSE or equivalent, High school or equivalent / A level or equivalent, Vocational degree, Bachelor's degree, Master's or professional degree, Doctorate degree, Other

Q1.4. Which country do you live in?

Q1.5. What is your current employment status?

- Options: Employed full-time, Employed part-time, Other, Prefer not to answer

Q1.6. What is your current job title?

Q1.7. How many years have you worked with or in the healthcare industry?

Q1.8. Have you been trained in IT security as part of your degree program, apprenticeship or further training?

- Options: No, Unsure, Yes, Prefer not to answer

Q1.9. Do you have any questions or comments you would like to make?

B INTERVIEW GUIDE

Procurement.

(1) I would now like to talk to you about a specific case. I'm interested in learning about how IoT devices are procured, integrated, and maintained in terms of security.
(2) Can you tell me about a case where you ordered and integrated something related to IoT in a hospital?
(3) What was the reason for the purchase?
(4) Who was the initiator for the procurement?
(5) What influence did you have in purchasing the device?
(6) Did you have the opportunity to bring in your requirements (e.g. compatibility requirements or similar)?
(7) What requirements were there for this device or for the related software?
(8) Were there requirements for the security of the devices?
(9) Where did these come from?
(10) In your opinion, are there any security requirements that have been ignored or not fully met?
(11) Why is that?)
(12) Why is that?
(13) If you now think back to other orders, was the issue of security dealt with differently there?

Integration and Maintenance.

(1) How did you go about integrating the new device?
(2) Who was involved?
(3) How did you go about security?
(4) Did you have any problems?
(5) How did you solve them?
(6) Did you have specific security requirements regarding the integration of the device?
(7) Did these security requirements differ from other IT devices?
(8) Did you get support (e.g. from the manufacturer)?
(9) How exactly did this happen?
(10) What does the integration between different devices from different manufacturers look like?
(11) Are there any problems or challenges regarding that?
(12) How did this work with other devices? Was it done differently there?
(13) Who is responsible for maintenance / patches / updates?
(14) What is the procedure here?
(15) What role does the manufacturer play?
(16) How often do you get updates & patches?
(17) Were there ever security warnings or recommendations from the manufacturer?
(18) Do you give feedback to the manufacturers regarding security issues?
(19) Do you feel sufficiently supported by the manufacturers?
(20) Have you ever had a security incident?
(21) How did you deal with it?
(22) If anything was possible, what would you like to see from the manufacturers in terms of security?

Usage.

(1) Who is using the device?
(2) What does the user interaction with the device roughly look like?
(3) What exactly does security look like for the end user?
(4) How is it ensured that no unauthorized person can gain access to the devices?
(5) Have there ever been any problems?

(6) How well do end users handle the security components of the devices?
(7) Who do users turn to when they have problems?
(8) How do you secure the administrative access to IoT devices?
(9) What does that look like with other devices?
(10) Do all employees follow the security rules?
(11) Is security sometimes bypassed?
(12) Why do you think this happens?
(13) Does the management or those responsible for security know about it?
(14) Is there a training process in place that addresses the security components of the IOT product?

Attitudes.

(1) How do you think usability and security are related?
(2) Are they related at all?
(3) Imagine a major security vulnerability is found in an IoT device, how likely do you think this case is? / ... that the case will happen again?
(4) What could have led to this?
(5) Who would you hold accountable for this?
(6) How would this problem be dealt with? / What would the resolution process look like?
(7) In your opinion, is enough being done for security in relation to IoT?
(8) Why? Why not?
(9) Where does it fail?
(10) What should be improved?
(11) Are you getting enough resources for that?
(12) How do your coworkers see it?
(13) Do you talk enough about security as a team?
(14) Who do you think is responsible for security?
(15) How do you see your role in terms of security?
(16) If you look again at the measures for security in the IoT area and the resources you get for them: How important do you think security is to management?
(17) In conclusion to your interview, what would you like to share with management about security?
(18) Is there anything you would like to see on the topic of security?

C CODE BOOK

Table 2: Code book

Code	Description	Example Quote
Procurement	Statements that relate to the procurement process and are or could be related to security. These include influences on procurement, requirements, responsibility, etc.	*So in the context of procurement processes, before the procurement takes place, we had always tried to address this issue of security, whereas this is actually a difficult issue. (P7)*
Integration & maintenance	Statements that relate to the integration and maintenance process and are or could be related to security. These include influences on integration and maintenance, requirements, responsibilities, issues, vendor support, etc.	*Yes, most solution processes are updates, firmware updates, software updates. That's actually where most of the problems can be solved. Rarely do you have to get to the hardware. (P4)*
Usage	Statements that relate to the use of IoT devices and are or could be related to security. These include influences on the use, requirements, responsibility, problems, etc.	*It just happens out of the necessity of routine and necessary action because the primary focus is on the safety of the patient and you don't associate that might be at risk from unsafe use of technical devices. (P8)*
Technical Challenges & Mitigations	Statements that relate to technical components of software or hardware and could have an impact on IT security. Statements regarding compatibility, networks, and data that relate to IT security are also included. No statements are captured that relate to general technical factors (e.g., "The IoT devices measure accurately.").	*So medical technology, that's generally - well, it's all about patient data, medical data. They are slow. [...] (P1)*
Organizational Security Challenges & Mitigations	–	
Organizational Processes & Routines	Statements that describe organizational processes or measures that have or could have an impact on security, but do not relate to user interaction with security. These include business processes, etc.	*Unfortunately, this is also the case with these IoT devices, so that it is then increasingly left to the actual nursing staff, or the departments try to get the know-how in. But this is an open topic. I think there is still a lot to be organized. (P4)*
Security Knowledge & Attitudes	Statements that describe attitudes or the extent of knowledge of employees or the organization in relation to security. No statements are recorded about employee attitudes or knowledge related to other topics (e.g., "Employees receive training on how to log patient data").	*There is still a lot of ignorance about this topic. (P4)*
Organizational Relationships	Statements that represent relationships between employees in the organization, between organizations, or with external entities (not manufacturers or law) that have or could have an impact on security. Example: reputation. Statements that relate to communication between employees, etc. are also coded.	*Because I think the two worlds communicate relatively little with each other. Everyone sees only his own area. (P3)*
Responsibility	Statements that represent individuals' responsibility or lack of responsibility for IT security. No statements are recorded that capture the responsibility of individuals on other topics (e.g., "The CEO does not feel responsible for hiring new employees").	*The problem I see here is that current security concepts are usually broken down to the last and weakest link, in the example we just had 'The nurse who wants to do her job'. The responsibility is just the same. (P2)*
Resources	Evaluative statements that relate to effects of existing or lacking resources in the organization that could directly or indirectly affect security.	*[...] Resources is actually also such a point. How many people are available to look after this entire system landscape. Of course, it's also a big point that you have enough resources with enough time to familiarize yourself with the systems. [...] (P7)*
Requirements	All concrete requirements that are imposed on a medical device. Not only security- and privacy-related. Statements that exclude specific requirements (e.g. "IT does not provide any requirements") are also recorded.	*No, there are actually no direct requirements. So, of course, it is important that the systems in interaction, data integrity, data security avoidably guarantee. (P3)*
Manufacturer & Security	All statements on how manufacturers deal with the topic of IT security. This also includes support, communication and feedback to manufacturers. No statements about manufacturers are recorded that are not directly or indirectly about IT security (e.g., "The manufacturer makes sure that the IoT devices are inexpensive").	*So from the manufacturers in the area of medical technology, medical products, I would say that there is little to no qualified support in the environment of information security. [...] (P8)*
Law, Regulations & Contracts	All legal and regulatory factors that could have an impact on the IT security of IoT devices. No statements on other topics are covered (e.g., "Legal conditions to use a blood pressure monitor").	*So the primary requirements come from the medical field, or also from medical technology, which, for example, concerns the certification of medical devices. (P7)*
Usability	All statements that relate to usability and have or could have an impact on security. These include technical usability aspects (e.g., "The usability of IoT devices is poor") and opinions on usability ("If something has high usability, security suffers").	*Usability often gets in the way. If I have poor usability, I can't necessarily enforce high security.[...] (P3)*
External Influences	All statements that refer to external influences that have occurred or could occur and that affect or could affect security, but are NOT the manufacturer or "Law, Regulations and Contracts" (for example: "Interest in patient data is increasing, this is a threat"). These include primarily risks and opportunities that affect the external world.	*At the moment, I'm actually interpreting all the activities that are going on there more from the perspective of: How do we not get cyber crime coming in from the outside somehow? (P8)*
Security Recommendations & Wishes	All statements that are clearly expressed as suggestions for improvement or wishes for how something should be changed that would have an impact on security and has not yet occurred. "Best practices" belong in the "Mitigations" categories. Keywords: "You should...", "I wish...", "This is how it should be...", "This is how something could be prevented..." It is not coded interpretively.	*[...] If then I would first say that there is monitoring on Critical Gaps from the manufacturer and they are actively coming at us to close those gaps.[...] (P1)*
Security Incidents	Statements in which specific security incidents are named that have occurred in the organization, could be averted, or possible security incidents are described. Consequences, causes and mitigations are also recorded. Only concrete examples are recorded and not interpreted. Important: must be coded with organizational, end-user or technical code categories.	*That's quite realistic, that happens all the time. You take this camera, the few times only noticed that this vulnerability was exploited but that there are major vulnerabilities discovered, especially in IoT devices, that is commonplace. It happens all the time. (P4)*