pHealth 2022
B. Blobel et al. (Eds.)

doi:10.3233/SHTI220977

Information Security Risk for Welfare Technology and Personal Healthcare Devices

Alvhild SKJELVIK[a,1] and Bian YANG[b]
[a] *Norwegian University of Science and Technology, Gjøvik, Norway*
[b] *NTNU, Gjøvik, Norway*

Abstract. Welfare technology is expected to become a larger and more important part of the healthcare sector. This creates a need to understand, which information security risks welfare technology and affiliated devices are exposed to. In a scoping review, we present an extensive overview of relevant threats. Furthermore, some key vulnerabilities in health technologies like IoMTs and welfare technology devices are highlighted. In the conclusions, the risks relevant for welfare technology is discussed, where four top risks are emphasized as a result of the findings.

Keywords. Information security, risk, threats, vulnerabilities, welfare technology, healthcare devices

Introduction

In the years coming, countries around the globe and especially European countries will be facing a demographic shift towards an aging and multi-diseased society as well as a massive resource scarcity in healthcare [1]. An example is the look at the Swedish population, were the part aged 80 is expected to increase from 5.3% in 2020 to 23% in 2030 [2]. In this context, it is argued that technology will become a solution to meet some of the predicted care-needs. New and innovative technological solutions can help taking over some of the care-work, especially related to less complicated medical tasks such as providing medication, home-based assistance, monitoring of vital signs, just to name a few [3]. For a long time, the healthcare sector has been dependent on technology to provide necessary care for patients, especially in hospitals and increasingly in home-based care. Medical devices in healthcare are not a new phenomenon, but the increasing amount of new solutions, systems, application and devices is changing how healthcare services are delivered. An increasing trend in the healthcare sector is the use of the Internet of Medical Things (IoMT), welfare technology and remote, distributed care solutions.

Research Motivation and Research Question

The integration of new technological solutions in healthcare imposes new risks. The IoMT industry alone is predicted to contain over 21 billion devices by 2025. From an information security and privacy perspective, there are risks that must be addressed to ensure the security and safety of health data, and ultimately of the patients. This paper

[1] Corresponding Author. Alvhild Skjelvik, Norwegian University of Science and Technology, Gjøvik, Norway; E-mail: Alvhild.skjelvik@ntnu.no.

explores the following question: *Q1: Which information security risks are relevant for welfare technology?*

Welfare technology is a term coined in the Nordic countries, and is similar to assisted living technology, ambient assisted living technology and IoMT to name a few. When exploring which risks that are relevant for welfare technology, one should also explore which threats and vulnerabilities welfare technologies and similar devices can be exposed to. This will help strengthening the understanding of how and which risks that can materialize.

1. Method

To complete this scoping review, a six-step method has been completed as suggested by [4]. The suggested steps is a straight-forward approach, where we searched through previous research that were using different methods, such as qualitative, experimental and mixed methods. A scoping review aims at understanding what current research exist related to the chosen topic [4]. When completing these six steps, suggestions by [5] on how to conduct a literature review was also included where appropriate. In step 2 of the approach suggested by [4], the Boolean logic as explained in [5] was used. Further, in step 3 of "selecting studies", we established inclusion and exclusion criteria as a guide to include relevant studies. In this paper we did not consult with stakeholders or relevant interest groups, but it is desired to do so in extension of this research.

To generate findings, searches were conducted in the following databases Science Direct, IEEE digital library, ACM digital Library, PubMed, Web of Science and AIS electronic library. The following search words were used to generate findings: "welfare technology", "telecare", "telemedicine", " IoMT", "assisted living technologies" AND "security", AND "Risk", AND "security risk". A total of 9 searches was performed, resulting in an total number of 2193 findings. Literature relating to the importance of information security for welfare technology is scarce. To include papers relevant for welfare technology, inclusion and exclusion criteria were established. These are presented in Table 1.

Table 1. Inclusion and exclusion criteria

Inclusion	Exclusion
Peer reviewed journal or conference paper	All other excluded
Published in English or Norwegian	All other languages excluded
Topic focusing on information security risks, threats or vulnerabilities relevant for welfare technology	Papers focusing on specific security mechanisms e.g. biometric solutions, blockchain
Research object healthcare sector	All other sectors excluded
Healthcare technologies suited definition of welfare technology[6]	All other technology excluded

A large number of findings were identified in the first search (N=2193). Through the first screening, this number was reduced to 58 papers. Following the first screening, a second screening was performed, where the inclusion and exclusion criteria's were used. During the second screening every paper was read back-to-back, resulting in 5 additional papers being identified as relevant through the snowballing method. When the first screening, second screening and the snowballing method was completed, a total of 22 papers were included in this review.

2. Results

In this section, relevant findings will be presented. We will start by presenting relevant threats, attacks and vulnerabilities. Thereafter, identified risks will be discussed.

2.1. Threats and vulnerabilities

According to [7], IoMT devices can be divided into four categories: wearable devices, implantable devices, ambient devices and stationary devices. Devices operate at different layers of the system architecture, where each layer is exposed to threats in different ways, and can be subjected to different types of attacks. Further, [8] refers to the FDA stating that for every 1000 connected device, roughly 164 attacks threaten them. [9] found devices depending on wireless personal area networks through Bluetooth-low-energy to be more exposed to Man-in-the-Middle attacks, replay attacks and network communication decryption as a result of insufficient encryption schemes. Thus, [9] uses information security principles by first reviewing how DDoS may jeopardize availability of implantable devices, and second how replay attacks can compromise confidentiality and integrity. Similarly, [10] refers to security principles when reviewing relevant threats for personal medical devices, where [11] identified over 50 different threats related to the security principles, mapped against different stages of data transmission. Threats towards confidentiality were evaluated to be the most serious.

In [12] several known attacks are highlighted. Similar to [7] and [9] the different layers of the IoMT system architecture is considered, as layers have different impacts on the data collection, transmission and storage. [12] highlight IoMT system risks and specific attacks that can threaten IoMT devices, such as physical attacks and network attacks. The most frequently mentioned network attack is DDoS, MITM, replay attack and brute force attack [12, 13, 14, 15] reviews the threat and vulnerability landscape for IoMT, where cardiac devices, implantable brain devices and pacemakers are examined. The authors stress the potential of blind and targeted attacks. When [16] explores living-labs it is emphasized that threat actors may be more inclined to attack these environments as it is a low-risk and high-reward attack. Thus, the vulnerabilities in these digital ecosystems are argued to be many. IoMTs have less security mechanisms than a laptop, which makes them more vulnerable of attacks. [17] divides telemedicine security threats into seven specific areas, where each threat area represents a point where threat actors can compromise assets through common vulnerabilities – resulting in multiple risks for telehealth care systems.

[18] states that the healthcare sector is more vulnerable of attacks due to the high value of data being processed. This is supported by [14] who found threats towards IoMT devices to be much higher when health data was processed. Further, [14] finds several easily exploitable vulnerabilities in sensors, as security measures are light-weight due to constrains such as small storage space and low battery capacity. Another factor that introduce vulnerabilities is network connectivity. When connecting devices to a network, both the attack surface and potential vulnerabilities increase [14]. Similarly, [19]

emphasize that devices connected to network increases vulnerabilities as they become endpoints or access points for attacks.

2.2. Information security risks

In [20] it is highlighted that downtime in healthcare devices can lead to patient harm or in worst case death. [13] refers to solution providers to provide security, and argues that though providers offer similar security mechanisms, they differ in the protection they provide. Besides, it can contribute to increase complexity of the device landscape, as different devices serve different purposes, offer different functionality and ultimately have different needs for security. As stated in [13] "each type of device poses its own security risk". This is supported by [21] who expresses a great concern that welfare technology will be a security risk for patients.

[22] explores sensors and smart homes for elderly in healthcare, where one of the key concerns of using devices is related to security. Alike [7, 8] find that the most common risk for IoMTs can be associated with complexity and inconsistency of devices. Similar to [22], the use of welfare technology for elderly in a homecare setting is examined in [23]. A risk that prevailed in this study was the dependency of healthcare workers to perform certain tasks such as charging devices, turning on alarms, sensors and so forth. Third-party risks are also mentioned, especially in cases when dependent on assistance from vendors/suppliers [23]. [24] stresses risks related to supply-chain, network security and privacy. Further, [10] highlights device security, connectivity security and cloud security as three security areas with higher risk exposure.

In [25], the authors stress the security of mobile devices in telehealth systems. Further, the current trend in software development related to increased connectivity and an exponential growth in medical data contributes to a high risk exposure for the telehealth system and affiliated devices [25]. Specific risks associated with hacking and remote monitoring, data availability, unauthorized access, unauthorized traffic monitoring and third-party intrusion were identified by [26], who views the risks related to IoMT as high. In [27] risk is connected not only to technology, but also to human factors such as how humans interact with technology, their knowledge and their competence. Hence, [17] finds that ICT competence have effect on security, which ultimately makes telemedicine highly prone to cyberattacks.

3. Discussion

Several threats, vulnerabilities and risks has been identified in this review. There is an inherent risk in welfare technologies as they are exposed to different risks by serving different purposes. Especially considering that compromise of welfare technology have different consequences for patients depending on the function of the device [14][16]. In the following, four top risks identified as relevant for welfare technology will be discussed.

Literature demonstrates the once technology is connected to internet, the potential risk increases due to an increase in attack surface. Meaning that devices that are connected to either share or transfer information through network connectivity can be more vulnerable towards cyber threats [12, 14, 15, 16, 18, 19, 20, 22]. In a future scenario where healthcare services rely on welfare technology, the consequences if a risk materializes increases [28]. Also, imagining a closer interconnectivity between welfare technologies, IoMTs and medical devices will introduce new risks [15, 16]. Currently, there are several known risks related to medical devices, like those for pacemakers, implantable cardiac devices and insulin pumps [9, 14, 19]. These risks exist even though medical devices are regulated. For welfare technologies and affiliated devices, there is no standardization framework nor regulation to ensure the security of devices [16].

In the field of security, the human factor is often viewed as the weakest link as they can be manipulated. In several papers, the human factor is of importance when it comes to information security breaches and use of technology [7, 11, 23, 28]. [28] claims that during the Covid-19 pandemic, 86% of the attacks was affiliated with phishing, i.e. humans being exploited. [23] stated that training healthcare workers AND users (e.g. elderly using welfare technology) will increase a sense of safety and mitigate the chance of patients getting hurt due to errors. Meaning that if the training and awareness is sufficient, the information security risk can actually be reduced.

Several different manufacturers, producers, developers and so forth is a common factor for different health technologies, IoMTs, welfare technologies and personalized devices. There can be multiple third-parties involved, with varying focus on security. Both [14] and [16] emphasize that there is a lack of insight into the consequence of security risks, as they can lead to disruption of normal operations. Further, a concern expressed in several papers related to the inadequate security at the device level, such as insufficient encryption schemes [27]. This poses a serious risk for welfare technologies [10, 13, 23, 24]. Many different third-parties can be challenging to manage and follow-up to ensure sufficient security, which in turn can result in higher risk exposure.

Complexity is the forth risk and is addressed in several papers, as it can create a intertwined technological ecosystem which can be difficult to manage [7, 20, 22, 23].This is relevant for welfare technology, especially when viewing available technologies and potential threats towards different devices. Complexity in the technological ecosystem-, available devices-, number of manufactures-, number of devices being used interchangeably-, and interconnectivity between devices, is a risk that based on this review, is likely to increase. Therefore, complexity is evaluated to be a highly relevant risk for welfare technology.

4. Conclusion

Information security risks will likely continue to exist for welfare technology. Some would even argue that without risks - we are not progressing. However, one must understand the risk, especially in the healthcare sector where risks may have fatal consequences. This paper has identified threats, vulnerabilities and several information security risks relevant for welfare technology. The top four relevant risks identified is network connectivity, human factors, third-party risks and complexity.

There is an inherent risk in the unregulated, free-marked devices, as there is not a guarantee for their security and henceforward safety for patients. Several more questions should be researched further to ensure security and trustworthiness of welfare technology and devices. Currently, lacking eligibility criteria and standardization of the free market, allows unserious actors to produce devices with insufficient security and possibly at risk of attacks. This contributes to a urgency to gather and disseminate knowledge about information security risks relevant for welfare technology and related devices. Thus, it demonstrates a need for standardization and focus on built-in security mechanisms.

References

[1] Spekter. Morgendagens helseutfordringer – behov for en velferdsmiks. Omsorgsutvalgets rapport 2019.

[2] Cozza M, Crevania L, Hallina A, & Schaeffer J. Future ageing: Welfare technology practice for our future older selves. Futures. 2019;109:117-129.

[3] Brendel F, Einhaus L, Then F. Resource scarcity and prioritization decisions in medical care: A lab experiment with heterogenous patient types. Health Economics. 2020;30(2):470-477.

[4] Arksey H, O'Malley L. Scoping studies: towards a methodological framework. International Journal of Social Research Methodology. 2005;8(1):13-32. DOI: 10.1080713645570320001196l6

[5] Fink A. Conducting Research Literature Reviews: From the Internet to Paper. (2nd ed.). Sage Pu. (2020)

[6] Woll A. Use of Welfare Technology in Elderly Care (PhD Dissertation). University of Oslo 2017.

[7] Alsubaei F, Abuhussein A, et al. Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment. 2017 IEEE 42nd Conference on Local Computer Networks Workshops.

[8] Aljumaie SG, Alzeer GH, Alghamdi RK, Alsuwat H, Alsuwat E. Modern Study on Internet of Medical Things (IOMT) Security. IJCSNS. 2021;21(8).

[9] Kandasmy K, Srinivas S, Achuthan K, Rangan VP. IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. Journal on Information Security 2020;8.

[10] Hatzivisilis G, Soulatos O, et al. Review of security and privacy for the internet of medical things (IoMT): Resolving the protection concerns for the novel circular economy bioinformatics. 15th international Conference of Distributed Computing in sensor systems. Santorini, Greece, 2019, May, 29-31.

[11] Henriksen E, Burkow TM, Johnsen E, Vognild LK. Privacy and information security risks in a technology platform for home-based chronic disease rehabilitation and education. BMC Med Inform Decis Mak 2013 Aug 9;13:85.

[12] Ghubaish A, Salman T, Zolanvari M, Unal D, Al-Ali A, Jain R. Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security. IEEE internet of things, 2021;8(11).

[13] Alsubaei F, Abuhussein A, Shiva S. Ontology-Based Security Recommendation for the Internet of Medical Things. IEEE Access. 2019;7.

[14] Sun Y, Lo FPW, Lo B. Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey. IEEE Access. 2019;7.

[15] McGowan A, Sittig S, Andel T. Medical internet of things: a survey of the current threat and vulnerability landscape.54th Hawaii International Conference on System Science. Kauai, USA, January 05.

[16] Kioskli K, Fotis T, Mouratidis H. The landscape of cybersecurity vulnerabilities and challenges in healthcare: Security standards and paradigm shift recommendations. ARES 2021. Vienna, Austria, 2021, August, 17-20.

[17] Kim DW, Choi JY, Han KH. Risk management-based security evaluation model for telemedicine systems. BMC Medical informatics and decision making. 2020;20(106).

[18] Sangpetch O, Sangpetch A. Security context framework for distributed healthcare IoT platform. HealthyIoT 2016. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. 2016;187. https://doi.org/10.1007/978-3-319-51234-1_11

[19] Michele RD, Furini M. IoT Healthcare: Benefits, Issues and Challenges. GoodTechs 19, Valencia, Spain, 2019, September, 25-27.

[20] Mushtaq M, Shah MA, Ghafoor A. The internet of medical things (IOMT). Security threats and issues affecting digital economy. CADE 2021. Online conference, 2021, June, 02-03.

[21] Nilsen ER, Dugstad J, Eide H, Gullslett MK, Eide T. Exploring resistance to implementation of welfare technology in municipal healthcare services – a longitudinal case study. BMC Health services research. 2016;16 (657).

[22] Maujumder S, Aghayi E, Noferesti M, Memarszadeh-Theran H, Mondal, T., Pang, Z. & Deen, M.J. (2017). Smart homes for elderly healthcare – recent advances and research challenges. Sensors 2017; 17(11), 2496.

[23] Johannessen TB, Holm AL, Storm M. Trygg og sikker bruk av velferdsteknologi i hjemmebasert helse- og omsorgstjeneste. Tidsskrift for omsorgsforskning. 2019;5(3): 71-83.

[24] Tarikere S, Donner I, Woods D. Diagnosing a healthcare cybersecurity crisis: The impact of IoMT advancements and 5G. Business horizons. 2021;64(6):799-807.

[25] Márques G, Astrudillo H, Tarmasco C. Exploring security issues in telehealth systems. 1st international workshop on software engineering for healthcare (SHE-19), Montreal, Canada, 2019, May, 27-29.

[26] Somasundaram R, Thirugnanam M. Review of security challenges in healthcare internet of things. Wireless Networks. 2021;27:5503-5509.

[27] Parsons EKI, Panaousis E, Loukas G. How Secure is Home: Assessing Human Susceptibility to IoT Threats. Association for Computing Machinery. PCI 2020, Athens, Greece, 2020. November, 20-22.

[28] Hathaliya JJ, Tanwar S. An exhaustive survey on security and privacy issues in Healthcare 4.0. Computer Communications March 2020;153:311-335.