Cyber(in)security of medical devices

Erik Kamenjašević, KU Leuven Centre for IT & IP Law, Belgium

Elisabetta Biasin, KU Leuven Centre for IT & IP Law, Belgium

Abstract

Cyberattacks on healthcare institutions and medical devices that have increasingly occurred during the coronavirus pandemic reaffirmed the importance and urgency of ensuring cybersecurity in the healthcare sector. One such attack may have economic, material, and life-threatening consequences for patients already in a vulnerable situation. This paper focuses on the cyber(in)security of medical devices by analysing this issue in the context of the UN SDG 3 as well as supranational, trans-governmental and national initiatives concerned with medical devices cybersecurity.

Introduction

Cybersecurity of medical devices has become a concrete concern for regulators and policymakers across the globe. Following the coronavirus pandemic, there has been an increase in cyberattacks on critical healthcare infrastructures, which have put patients' health and safety at risk. For example, such cyberattacks involved connected medical devices as part of healthcare IT systems and medical devices that patients carry or wear, such as insulin pumps.

A successful cyberattack could impact the healthcare system's access and availability, causing delays and disruptions in healthcare services. The unavailability of services may have fatal consequences when patients' critical health conditions require immediate hospitalisation, thus creating an overall cyber(in)security within a healthcare system.

The increase in cybersecurity risks for medical devices has led legislators and regulatory bodies to pay more attention to medical devices' cybersecurity. Research by legal doctrine is critical to support policymakers in addressing their legal and regulatory challenges.

In this view, this paper addresses the regulatory initiatives by the USA and EU, the trans-governmental initiatives from the IMDRF and several national initiatives (including Japan, Germany, Singapore, France, Canada, Australia, Saudi Arabia, Brazil and China) dealing with medical devices' cybersecurity. Through this analysis, the paper provides recommendations for lawmakers and policymakers on global, regional, national and local levels for tackling the growing cybersecurity risks, which could limit, distort or prevent access to quality essential healthcare services.

Medical device cybersecurity and the UN SDG 3

The UN Sustainable Development Goal (SDG) 3 aims to ensure healthy lives and well-being for all at all ages. More precisely, target 3.8 points at universal health coverage, including financial risk protection, access to quality essential healthcare services and access to safe, effective, quality and affordable essential medicines and vaccines for all.

If manufacturers and other stakeholders[1] involved in developing and deploying connected medical devices (such as AI-based medical devices, among others) do not implement the necessary measures to mitigate possible cybersecurity-related risks, these medical devices may become vulnerable to cyberattacks.

For example, an AI insulin pump under a cyberattack involving the poisoning of data sets or extraction of data[2] could stop working correctly and provoke serious health risks to the patient using it.[3]

Cyberattacks on medical devices could also provoke indirect consequences. These could include diminishing patients' trust in the security of the healthcare system, fear and hesitancy towards using these medical devices due to their cyber(in)security-related consequences.[4]

[1] E. Biasin, E. Kamenjašević, *Cybersecurity of Medical Devices. Regulatory Challenges in the European Union*. In: I. Cohen, T. Minssen, W. Price II, C. Robertson, & C. Shachar (Eds.), *The Future of Medical Device Regulation: Innovation and Protection*, pp. 51-62, 2022, Cambridge University Press, doi:10.1017/9781108975452.005.

[2] E. Biasin et al., *Cybersecurity of AI medical devices: risks, legislation, and challenges*. In: B. Solaiman, I. Cohen (Eds.), *Research Handbook on Health, AI and the Law,* forthcoming 2023, Edward Elgar Publishing Ltd.

[3] T. Levy-Loboda et al., *Personalized Insulin Dose Manipulation Attack and Its Detection Using Interval-Based Temporal Patterns and Machine Learning Algorithms*, 2022, Journal of Biomedical Informatics.

[4] E. Biasin, E. Kamenjašević, *Cybersecurity of medical devices: new challenges arising from the AI Act and NIS 2 Directive proposals,* 2022, International Cybersecurity Law Review, doi.org/10.1365/s43439-022-00054-x.

Without a strong element of trust in the healthcare sector and within the doctor-patient relationship, ensuring the quality of care is challenging. Ultimately, this can negatively affect SDG 3 by limiting people's access to healthcare services having an appropriate cybersecurity standard and preventing them from accessing safe medical devices. Furthermore, cybersecurity vulnerabilities could induce healthcare providers and patients extra financial costs, thus additionally burdening those who already find themselves in vulnerable circumstances.

Regulatory guidance on medical devices cybersecurity

National regulatory authorities have demonstrated increasing interest in medical device cybersecurity throughout the last decade through guidance documentation. One of the first regulatory experiences dates back to 2005 when the US FDA's Centre for Devices and Radiological Health (CDRH) was among the first authorities to publish documents relevant to medical device cybersecurity (FDA, 2005), dealing with the content of premarket submissions and quality systems considerations (FDA, 2014; 2018; 2022), postmarket (FDA, 2016) and off-the-shelf software (FDA, 2018) requirements.

The first guidance dealing with medical devices cybersecurity requirements embedded in the EU Medical Devices Regulation (MDR)[5] was issued in 2019 by the European Commission's Medical Devices Coordination Group (MDCG)[6]. This non-binding soft-law document represents an essential step in the EU.

In 2015 the Japanese Pharmaceutical and Medical Devices Agency developed its first documentation on Ensuring Cyber Security of Medical Devices in 2015 (PMDA, 2015), followed by more recent updates in 2018 and 2022 (PMDA, 2018; 2022). In 2017, China had its Medical Device Network Security Registration on Technical Review Guidance Principle (IMDRF, 2020). In 2018, Germany's Federal Office for Information Security released its Cyber Security Requirements for Network-Connected Medical Devices (BSI, 2018), followed by Singapore's Standard Council's technical references on Medical device cybersecurity (SSC, 2018). In 2019, the French authority had its guidelines on the cybersecurity of medical devices integrating software during their life cycle; (ANSM, 2019), followed by Health Canada's Premarket Requirements for Medical Device Cybersecurity (Health Canada, 2019). In 2019, the Australian Department of Health and Aged Care – Therapeutic Goods Administrations released guidance documentation (TGA, 2019, amended throughout the years) consisting of three documents dealing with consumer information, guidance for industry, and information for users. Brazil's health authority published its principles and practices on medical device cybersecurity in 2020. (ENVISA, 2020). Saudi Arabia is drafting other ongoing initiatives involving upcoming guidance (SFDA, 2019).

Trans-governmental regulatory guidance on medical devices cybersecurity

The International Medical Device Regulatory Forum (IMDRF) is the most comprehensive trans-governmental initiative. The IMDRF is a voluntary group of medical device regulators that aims to accelerate international medical device regulatory harmonisation and convergence.[7]

In 2020, the IMDRF published its Principles and Practices for Medical Devices Cybersecurity. In 2022, the IMDRF released for public consultation the Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity (IMDRF, 2022). This guidance represents a positive step forward in recognising the importance of medical device cybersecurity at an international level. Another important piece of guidance concerns legacy medical devices.[8] This document is planned to be released in its final version in 2023.[9] The guidance is oriented at providing instructions for the safe use of legacy devices, so it is expected to play a role in sustainability by

[5] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017, on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, 2017 O.J. (L 117/1).

[6] European Commission, Medical Devices Coordination Group, *Guidance on Cybersecurity of medical devices*, 2019.

[7] The members of the forum include Australia, Brazil, Canada, China, Europe, Japan, Russia, Singapore, South Korea, the UK, USA. The IMDRF official observers are the World Health Organisation and Argentina. Other international entities, regional organisations or affiliate organisations may take part in the IMDRF meetings as 'Regional Harmonisation Initiatives', which include the Pan American Health Organization (PAHO), the APE LDIF Regulatory Harmonisation Steering Committee, and the Global Harmonization Working Party (GHWP). Official and invited observers, as well as regional harmonisation initiatives may participate to the IMDRF management committee meetings, but they do not participate in the decision making process (IMDRF, 2023).

[8] Legacy medical devices are those that – for different reasons, e.g., are 'too old' to be updated – cannot be protected against current cybersecurity threats.

[9] See https://www.imdrf.org/sites/default/files/2022-09/MDCG.pdf.

supporting their use or re-purposing them while ensuring patients' safety.

International experiences: opportunities for the WHO

Since the start of the COVID-19 pandemic, the WHO has signalled a dramatic increase in cyberattacks directed at its staff (WHO, 2020). Besides concise guidance on how to avoid phishing attacks, the Organisation did not show relevant concern about cybersecurity issues in healthcare as a whole. However, the WHO has issued guidance on the ethics and governance of artificial intelligence for health (WHO, 2020), a report produced by two departments in the Science Division: Digital Health and Innovation and Research for Health. The report mentions cybersecurity threats for AI health systems in a short paragraph. Awareness of and preparedness for this specific issue must be discussed globally.

Beyond regulatory initiatives: standardisation and harmonisation

Where no regulatory guidance or cybersecurity-specific laws are in place or do not cover certain cybersecurity-related aspects appropriately, standards may play a role in ensuring a common level of cybersecurity for medical devices. There are many security standards, such as those issued by ISO, IEC, and NIST.[10] In the last years, some working groups (ISO TC215, IEC SC62A) at the IEC and ISO identified the need to work on a medical device software-specific standard.[11] Another referenced standard on medical device cybersecurity is the AAMI's Principles for Medical Device Security – Risk Management (2019).

Those standards may contribute not only to SDG 3 but also to SDG 9 (build resilient infrastructure, promote inclusive and sustainable industrialisation and foster innovation), SDG 10 (reduce inequality within and among countries), and SDG 12 (ensure sustainable consumption and production patterns).[12]

However, the main shortcoming is the economic barrier to their access. Such barriers may negatively affect the possibility for stakeholders (such as healthcare providers or manufacturers) to enhance their knowledge and tools, thus ensuring an appropriate level of cybersecurity for their services and devices.

Conclusion and recommendations

The UN Report to the Commission on Human Rights (UN, 1974) expressed the need for more medical data security in the healthcare sector. With this warning, the UN has already paved the way for addressing cybersecurity as a global concern, requiring the simultaneous involvement of stakeholders from around the globe.

Below we propose our main recommendations that should be addressed with no delay on global, regional, national and local levels:

Global level: the WHO should give more relevance to the issue of cybersecurity and play an essential role in preparing a comprehensive digital health guidance document, including cybersecurity of healthcare systems from ethical, legal, technical and societal perspectives. To raise awareness among different stakeholders[13] at all levels of a cybersecurity chain (including healthcare providers, healthcare professionals, device manufacturers, IT providers and IT operators within the supply chain, users and patients) the WHO should develop elaborated and practical policies and global strategies.

Regional level: the initiatives taken by the IMDRF, as a unique forum comprising many countries where common cybersecurity solutions can be discussed, represent good trans-governmental practice. Its work must be continued with ongoing updates of guidelines. Future guidance should focus on new questions concerned with medical device cybersecurity. These should consider, for instance, cybersecurity-specific aspects of AI-based medical devices or cybersecurity of medical device health data sharing.

National level: national authorities should collaborate and build upon each other's knowledge and guidance. Where no guidance exists yet, national regulatory agencies should consider cybersecurity as a core

[10] See e.g., the ISO 27000s to the IEC 62443 series on industrial control Systems, to the NIST Cybersecurity Framework.

[11] These resulted, for instance, in the IEC 81001-5-1:2021 standard on health software and health IT systems safety, effectiveness and security (IEC, 2021).

[12] See https://www.iso.org/standard/76097.html.

[13] E. Kamenjašević, D. Fabcic Povse, *A Data Protection Perspective on Training in the mHealth Sector*. In: G. Andreoni et al. (Eds.), *m_Health Current and Future Applications*, pp. 71-85, 2019, EAI/Springer Innovations in Communication and Computing. Springer, doi.org/10.1007/978-3-030-02182-5 5. Since cybersecurity is a joint responsibility involving various stakeholders – which are often located in different territories – the WHO is best suited to provide examples on matters insisting on the healthcare cybersecurity chain and which involve healthcare providers, professionals, manufacturers, IT providers and operators within the supply chain, users and patients.

element in their regulatory agenda and draft thematic guidance for it. Where adopted, national regulation agencies' guidance should target the different actors of a cybersecurity chain and set tailored requirements for them based on their roles and responsibilities. In all cases, regulatory agencies should act as the main ideators of national healthcare cybersecurity awareness initiatives and education.

Local level: healthcare organisations should share common cybersecurity best practices and train their healthcare and other personnel with personalised and recurrent cybersecurity training. Apart from educational purposes, such training should help organisations to understand where the cyber threats are coming from, to measure the actual risk and find effective mitigative measures.

Acknowledgments

The research by Kamenjašević and Biasin was carried out in the context of the Stanford Law School's Transatlantic Technology Law Forum Fellowship.

References

AAMI. AMI TIR57:2016 (R2019) Principles For Medical Device Security - Risk Management. (2019).

ANSM (Draft): Cybersecurity of medical devices integrating software during their life cycle. (2019).

Biasin E et al., 'Cybersecurity of AI medical devices: risks, legislation, and challenges'. In: B. Solaiman, I. Cohen (Eds.), Research Handbook on Health, AI and the Law, forthcoming 2023, Edward Elgar Publishing Ltd.

Biasin E, Kamenjašević E, 'Cybersecurity of medical devices: new challenges arising from the AI Act and NIS 2 Directive proposals', 2022, International Cybersecurity Law Review, 163.

Biasin E, Kamenjašević E, 'Cybersecurity of Medical Devices. Regulatory Challenges in the European Union'. In: I. Cohen, T. Minssen, W. Price II, C. Robertson, & C. Shachar (Eds.), The Future of Medical Device Regulation: Innovation and Protection, 2022, Cambridge: Cambridge University Press.

BSI, Cyber Security Requirements for Network-Connected Medical Devices (2018).

ENVISA, Princípios e práticas de cibersegurança em dispositivos médicos. (2020).

FDA, Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software. (2005)

FDA, Content of Premarket Submissions for Management of Cybersecurity in Medical Devices. (2014).

FDA, Content of Premarket Submissions for Management of Cybersecurity in Medical Devices. (2018).

FDA, Postmarket Management of Cybersecurity in Medical Devices. (2016)

FDA, Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions, (2022).

Health Canada, Premarket Requirements for Medical Device Cybersecurity (2019).

IEC, IEC 81001-5-1:2021 Health software and health IT systems safety, effectiveness and security — Part 5-1: Security — Activities in the product life cycle. (2021).

IMDRF, IMDRF Terms of Reference. (2023).

IMDRF, Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity. (2022).

Kamenjašević E, Fabcic Povse D, 'A Data Protection Perspective on Training in the mHealth Sector'. In: G. Andreoni et al. (Eds.), m_Health Current and Future Applications, 2019, EAI/Springer Innovations in Communication and Computing. Springer.

Levy-Loboda T, et al., 'Personalised Insulin Dose Manipulation Attack and Its Detection Using Interval-Based Temporal Patterns and Machine Learning Algorithms', 2022, Journal of Biomedical Informatics.

PMDA, Guidance on Ensuring Cyber Security of Medical Devices. (2018).

PMDA, Ensuring Cyber Security of Medical Devices. (2015).

PMDA, Strengthening Cyber Security Measures related to Medical Devices, etc. (2022).

Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017, on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, 2017 OJ (L 117/1).

SSC, Technical Reference n 67:2018. Connected medical device security. (2018).

TGA, Medical device cyber security guidance for industry, 2019.

TGA, Medical device cybersecurity – Consumer information. (2019).

TGA. Medical device cybersecurity information for users. (2019).

SFDA, Medical Devices Regulation and Requirements (SFDA Updates), Nov 14th 2019. (2019) http://www.ahwp.info/sites/default/files/Annex18_AHWP%20Member%20Country%20or%20Region%20Updates_Saudi%20Arabia.pdf

Sarewitz, D. and Nelson R., 2008, Three rules for technology fixes, Nature, 456

UN. Human rights and scientific and technological developments : uses of electronics which may affect the rights of the person and the limits which should be placed on such uses in a democratic society : report of the Secretary-General. (1974). https://digitallibrary.un.org/record/1629645