European Journal of Risk Regulation (2024), **15**, 872–875
doi:10.1017/err.2024.94

CAMBRIDGE UNIVERSITY PRESS

EDITORIAL

The Challenges of Cybersecurity in the Health Sector

Federica Casarosa[1,2] and Jaroslaw Greser[3,4]

[1]Scuola Superiore Sant'Anna, Pisa, Italy, [2]European University Institute, Firenze, Italy, [3]Warsaw Institute of Technology, Warsaw, Polland and [4]Vrije Universiteit Brussel (VUB), Brussels, Belgium
Corresponding author: Federica Casarosa; Email: Federica.casarosa@santannapisa.it

The digitalisation of the health sector is an ongoing phenomenon, which was only accelerated by the impact of the Covid-19 pandemic. Already in 2018, the European Commission addressed the priorities emerging in the digital transformation of health and care, identifying, first, the need to secure citizens' access to their health data (including across borders); secondly, the crucial importance of personalised medicine through shared European data infrastructure; third, the potential for citizen empowerment with digital tools for user feedback and person-centred care.[1]

Although the path seems set to enhance the possibilities to grasp the advantages of digital health and medicine, several challenges are emerging in this framework when looking at the cybersecurity of health devices, such as medical devices or more general Internet of Things devices that still collect data about users' health. Recent studies show that the health sector is among the sectors that are targeted by the highest number of attacks,[2] with at least twenty-six per cent of incidents reported across the period between 2021 and 2023.[3] Moreover, such security incidents have not only impacted the quality and the timely response of the health service, but they can also put patients' health at risk, if not their lives.[4] For instance, cases of ransomware attacks[5] reported in several EU countries have caused limited access to the Emergency Rooms and no access to patient medical records, cancellation of almost all non-emergency operations, and inaccessibility of hospital's business software, as well as medical imaging systems.[6] Although recent

[1] See EU Commission, Communication on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, COM(2018) 233 final.

[2] See ENISA, ENISA Threat Landscape: Health sector, 2023.

[3] Note that the cybersecurity incidents should be reported to the national competent authorities or to the Computer Security Incident Response Teams, pursuant art. 10 of Directive 2022/2555 of the European Parliament and the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation No 910/2014 and Directive 2018/1972, and repealing Directive (EU) 2016/1148, [2022] OJ L333/ 80.

[4] European Commission, Joint Research Centre, Reina, V. and Griesinger, C., Cyber security in the health and medicine sector: a study on available evidence of patient health consequences resulting from cyber incidents in healthcare settings, Publications Office of the European Union, Luxembourg, 2024, Available at <https://data.europa.eu/doi/10.2760/693487>.

[5] According to ENISA Threat Landscape for Ransomware Attacks, July 2022, a ransomware attack is a case where threat actors take control of a target's assets and demand a ransom in exchange for the return of the asset's availability and confidentiality.

[6] See EC-JRC, Cyber security in the health and medicine sector, 2024, p. 16–17.

research has not pointed to cases where the cyber attack directly leads to the serious deterioration of patients' health, this worst-case scenario cannot be overridden.

If, on the one hand, cybersecurity protection relies heavily on technological developments and research activity in computer science and engineering, on the other hand, legal interventions can enhance the level of awareness of such risks for individuals and companies and impose requirements and obligations aimed at preventing cyber incidents as well as ensuring resilience whenever such incidents cannot be foreseen and avoided.

This Special issue addresses the current legal framework that has been adopted so far by the European Union as regards cybersecurity issues in the health sector. The analysis will highlight that several legislative interventions overlap, addressing different perspectives. As anticipated above, a preliminary issue relates to the fact that more and more connected devices, such as the so called Internet of Things (IoT) devices, are used for medical and health purposes. Such IoT devices can be qualified as medical, according to the definition available in the Medical Device Regulation,[7] and therefore subject to the requirements and obligations defined therein; or they can have some e-health function, such as the possibility to check the heart rate of the user but are not qualified as medical devices. In this latter case, the mixed functions IoTs, as defined by **Gennari** in this Special issue, may be subject to different pieces of legislation, which do not always include a cybersecurity perspective. As **Biczysko-Pudełko** clarifies, the pre-contractual and contractual protection of users of such IoT devices is covered by several legislation falling into consumer protection law. In particular, an important improvement comes from the recently amended General Product Safety Regulation,[8] where the definition of a product also covers connected products and points to the fact that connected objects that affect the way another object works may pose a risk to product safety. Additionally, standard consumer protection legislation apply, requiring manufacturers to comply with information obligations and ensure fair contractual terms,[9] and protect consumers against unfair commercial practices.[10]

The framework becomes even more complex when looking at the liability perspective, where the recent Product Liability Directive Update (PLDU)[11] should be applicable. As **Gennari** shows, this legislation is extremely relevant regarding mixed functions IoT, as liability can be allocated to the manufacturer in case the defectiveness of the product is related to non-compliance with product safety requirements, including safety-relevant

[7] 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.

[8] Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC PE/79/2022/REV/1 [2023] OJ L 135/ 1.

[9] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council [2011] OJ L 304/ 64

[10] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council [2005]

OJ L 149/ 22.

[11] Directive of the European Parliament and of the Council on liability for defective products and repealing Council Directive 85/374/EEC. At the time of writing the text was adopted by the council but not yet published in the Official journal, the latest version is available at https://data.consilium.europa.eu/doc/document/PE-7-2024-INIT/en/pdf.

cybersecurity requirements. Still, coordination issues emerge when the IoT also embeds an artificial intelligence system, as in this case, the legislation applicable also includes the Artificial Intelligence Act,[12] as well as the proposed AI Civil Liability Directive. Although the application of the latter will be residual – applying only to "low-risk" AI systems – in case damage occurs, it will be difficult to demonstrate causation, as the claimant will need expert knowledge on the way in which algorithms work.

The use of artificial intelligence in medical devices has also been addressed by U.S. regulations. **Kamenesiak and Biasin** highlight that the historical roots of the regulatory play an important role in how the legislative interventions are framed. Their comparison between the European and the US approach shows that while the EU system is principle-based, the US one is a rule-based system reflecting a "command-and-control" approach. While the two approaches share the same risk-based systems, they have differences in device classification, centralization, premarket transparency, and device surveillance; such differences consequently impact the relevant rules from a cybersecurity perspective.

Another piece of legislation that will affect cybersecurity is the European Health Data Space Regulation (EHDS).[13] This legislation establishes a new data governance mechanism for primary and secondary use of electronic health data. While "primary use" refers to the processing of personal electronic health data for the provision of healthcare to the natural person to whom that data relates, "secondary use" refers to the reuse of personal and non-personal electronic health data for purposes other than the initial purposes for which they were collected or produced. Both aspects carry some critical elements that the proposed regulation cannot solve.

Looking at the primary use of data, **Casarosa**'s contribution highlights that the envisaged data space must ensure that the data are protected from cyber-attacks that may hamper data confidentiality, availability and integrity. Such measures are not only applicable to electronic health records but also to (interoperable) wellness devices and applications. Still, the measures listed in Annex I do not guarantee a sufficient level of protection in terms of security, which can only be tampered with by the coordinated application of the Cyber Resilience Act.[14] However, the interplay between these two legislative proposals may increase complexity, as in the case of serious security incidents, the manufacturer will have to notify two different authorities with different timelines and documentation required.

The rules applicable to the secondary use of health data are not without flaws too: first, the definitions of "personal electronic health data" and "non-personal electronic health data" within the EHDS are ambiguous; particularly, in the latter definition, there is no clear indication on how far it can cover the health status of natural persons or other healthcare-related information. In this case, **Rak**'s analysis shows that applying the concepts of "anonymisation" and "pseudonymisation" to electronic health data would be crucial. His analysis, moreover, highlights that an appropriate allocation of data protection responsibilities between data holders and health data access bodies is crucial to ensure alignment with data protection law and make secondary use of data secure by design, efficient and sustainable.

Another aspect of cybersecurity in the medical sector is the use of synthetic data to train medical AI. As **Greser** points out, there is no general prohibition on the use of this

[12] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on adapting non-contractual civil liability rules to artificial intelligence (AI Civil Liability Directive) COM/2022/496 final.

[13] Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space (henceforth: "EHDS"), compromise text. Available: https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=celex:52022PC0197.

[14] REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL 2024/2847 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) OJ L 2024/2847.

data; however, it must be subjected to a comprehensive risk assessment prior to each instance of its utilisation. Such an analysis should encompass two specific areas. The first area of concern is the quality and reliability of the databases used to create synthetic data, particularly when publicly available databases are employed to train the algorithms. In this case, the analysis should be conducted in terms of the possibility of an adversarial or other attack on the data, resulting in a malfunction of medical AI. The second area is to reject the assumption that synthetic data is anonymised. As research shows, in many cases it is possible to identify the identity of the individuals whose data was used to create synthetic data.

The contents of this issue illustrate the complexity and dynamism of the legal challenges related to cybersecurity in the medical sector. The situation is further complicated by the introduction of new technical solutions and global legal developments, particularly in the context of the regulation of artificial intelligence. Furthermore, the rising number of cyber threats to the medical sector and its growing vulnerability, which is directly proportional to the advancement of its digitalisation, must be acknowledged. It can be reasonably deduced that the role of lawyers specialising in cybersecurity within the medical sector will become more demanding, and consequently, the number of pertinent topics and proposed solutions will increase. The issue presented to our readers represents a contribution to this ongoing discourse, with the ultimate objective of enhancing the cybersecurity of the medical sector and optimising its functionality.

Financial support. The research was supported by PNRR project "SoBigData.it: Strengthening the Italian RI for Social Mining and Big Data Analytics" (Cambridge University Press B53C22001760006).

Cite this article: F Casarosa and J Greser (2024). "The Challenges of Cybersecurity in the Health Sector". *European Journal of Risk Regulation* **15**, 872–875. https://doi.org/10.1017/err.2024.94