Stanford – Vienna
Transatlantic Technology Law Forum

A joint initiative of
Stanford Law School and the University of Vienna School of Law

TTLF Working Papers

No. 108

Transatlantic Perspectives on AI-Based Medical Device Cybersecurity

White Paper

Erik Kamenjašević & Elisabetta Biasin

2023

TTLF Working Papers

Editors: Siegfried Fina, Mark Lemley, and Roland Vogl

About the TTLF Working Papers

TTLF's Working Paper Series presents original research on technology, and business-related law and policy issues of the European Union and the US. The objective of TTLF's Working Paper Series is to share "work in progress". The authors of the papers are solely responsible for the content of their contributions and may use the citation standards of their home country. The TTLF Working Papers can be found at http://ttlf.stanford.edu. Please also visit this website to learn more about TTLF's mission and activities.

If you should have any questions regarding the TTLF's Working Paper Series, please contact Vienna Law Professor Siegfried Fina, Stanford Law Professor Mark Lemley or Stanford LST Executive Director Roland Vogl at the

Stanford-Vienna Transatlantic Technology Law Forum
http://ttlf.stanford.edu

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

About the Authors

Erik Kamenjašević is a doctoral researcher at the KU Leuven Centre for IT & IP Law (CiTiP), a Transatlantic Technology Law Forum (TTLF) Fellow at Stanford University in 2022/2023, and a research fellow at the ISLC - Information Society Law Center at the University of Milano in 2023/2025. Erik was a visiting researcher at the Centre for Technology, Ethics, Law and Society (TELOS) at the King's College London in 2022/2023. Erik's doctoral research concerns ethical and legal issues associated with human mood enhancement technologies. The thesis aims to provide EU lawmakers with an analysis of the ethical issues and principles relevant to discussing these technologies in a regulatory context and an analysis of legal norms applicable to these technologies. Furthermore, Erik's research concerns fundamental rights, privacy, data protection, pharma laws, medical devices legislation, and cybersecurity in eHealth, AI, and ICT contexts. Erik published his research in the Philosophical Papers, the European Journal of Consumer Law, the European Pharmaceutical Law Review, the International Cybersecurity Law Review, with Cambridge University Press, and other journals, edited volumes, and books. Erik is a founding member of the Beyond Cosmethics IdeaLab. Before joining KU Leuven, Erik obtained a LL.M. in International Business Law from Vrije Universiteit Amsterdam (Netherlands) and a Master's degree in Law from the University of Rijeka (Croatia). Erik worked as a legal trainee in the Cabinet of the President of the EFTA Court, as a trainee lawyer-linguist at the Court of Justice of the European Union, and as a junior lawyer in a Croatian-based law firm.

Elisabetta Biasin is a doctoral researcher at the KU Leuven Centre for IT & IP Law (CiTiP), External Collaborating Expert on Data Protection of Big Data and Real-World Data at the European Medicines Agency (EMA), and Transatlantic Technology Law Forum (TTLF) Fellow at Stanford University in 2022/2023. In the 2023-2024, she was an Academic Visitor at the Centre for Health, Law and Emerging Technologies at the University of Oxford's Faculty of Law. Elisabetta's research concerns eHealth, AI, privacy and data, cybersecurity, In silico health and medical devices law. As part of her doctoral project ('Reconsidering the conceptualisation of accuracy as a principle of data processing'), she investigates the notion of accuracy in AI and data protection. Elisabetta published in the European Pharmaceutical Law Review, International Cybersecurity Law Review, Internet Policy Review, Cambridge University Press, and in other journals and edited collections. Previously to joining academia, Elisabetta worked as a Policy Intern at European Digital Rights (EDRi) and as a Junior Assistant at the Bolzano Criminal Court (Italy) and as a Data Protection Legal Advisor for Deloitte Legal Italy.

General Note about the Content

Suggested Citation

This TTLF Working Paper should be cited as:
Erik Kamenjasevic & Elisabetta Biasin, Transatlantic Perspectives on AI-Based Medical Device Cybersecurity: White Paper, Stanford-Vienna TTLF Working Paper No. 108, http://ttlf.stanford.edu.

Abstract

Cybersecurity of medical devices has become a concrete concern for regulators and policymakers in the US and EU. Following the COVID-19 pandemic, there has been an increase in cyber-attacks on critical healthcare infrastructures and their IT systems, which have suffered service disruptions and put patients' and other users' health and safety at risk. Recent studies and medical device manufacturers' disclosures have shown the potential safety risks of these types of vulnerabilities, including those of AI-based medical devices. Those could include data poisoning, data exfiltration, or even social engineering. The increase in cybersecurity risks for medical devices, exacerbated by the growing digitalization of healthcare services in the US and the EU, 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 White Paper addresses the legal and regulatory aspects of medical devices' cybersecurity and adopts a comparative perspective between the US and the EU. The regulation of medical devices in the EU has been historically inspired by the regulatory trends from the US, although with the different cultural, societal, and legal traditions that made them adapt to the specificities of the territory. Comparing the US and the EU legal landscapes concerning AI-based medical device cybersecurity means appraising their different regulatory systems. Therefore, this White Paper aims to answer the following research question*: what are the main implications of different regulatory approaches toward AI-based medical devices cybersecurity in the US and EU?*

Contents

Introduction

Cybersecurity of medical devices has become a concrete concern for regulators and policymakers in the US and EU. Following the COVID-19 pandemic, there has been an increase in cyber-attacks on critical healthcare infrastructures and their IT systems, which have suffered service disruptions and put patients' and other users' health and safety at risk.

Cyber-attacks on healthcare infrastructures may concern connected medical devices as part of their IT systems (for example, Picture Archiving Communicating Systems or medical imaging devices). Cyber-attacks could also concern medical devices that patients carry or wear, such as insulin pumps or pacemakers. A cyber-attack could impact healthcare systems availability, causing delays and disruptions in providing healthcare services. The unavailability of services may have fatal consequences when patients' critical health conditions require immediate hospitalization.

Unfortunately, these eventualities have already recurred in the past. For instance, during the Wannacry ransomware attack, thousands of appointments and operations were cancelled, and NHS patients "had to travel further to accident and emergency departments" (National Audit Office, UK Department of Health, 2018). In Dusseldorf, a hospital targeted by ransomware redirected a woman suffering from an aortic aneurysm to another emergency department 32 kilometres away. The distance delayed the patient's treatment by one hour, and she died shortly after (Ralston, 2020). Prosecutors tried to build the case by accusing hackers of negligent homicide, leveraging on a possible legal causation between the attack and the delay in treating the patient (id.).

Recent studies and medical device manufacturers' disclosures (FDA, 2022) have shown the potential safety risks of these types of vulnerabilities, including those of AI-based medical devices. Those could include data poisoning, data exfiltration, or even social engineering. (Biasin, Kamenjasevic, Ludvigsen, *forthcoming 2023*; Mozaffari-Kermani and others, 2015). For example, the poisoning of data used by AI-based medical devices could be considered a cyber-attack towards a medical device. In fact, once tampered with, a dataset could result in data unavailability, implying a data breach and possible disruptions in healthcare services. The same incident on the dataset could even lead the device to use erroneous data to generate predictions about one's health that, based on malicious sources, could lead to inaccuracies and thus threaten individuals' health.

The increase in cybersecurity risks for medical devices, exacerbated by the growing digitalization of healthcare services in the US and the EU, 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 White Paper addresses the legal and regulatory aspects of medical devices' cybersecurity and adopts a comparative transatlantic perspective between the US and the EU.

The regulation of medical devices in the EU has been historically inspired by the regulatory trends from the US, although with the different cultural, societal, and legal traditions that made them adapt to the specificities of the territory. Comparing the EU and the US legal landscapes concerning AI-based medical device cybersecurity means appraising their different regulatory systems. The US is a rule-based system reflecting a 'command-and-control' approach, while the EU system is a principle-based one (Wilkinson, 2021). While they share the main characteristic of being risk-regulation-

based systems, they have differences – for example, in device classification, centralization, premarket transparency, and device surveillance (Maak & Wylie, 2016), among others.

Therefore, this White Paper aims to provide insights into the main implications of different regulatory approaches toward AI-based medical device cybersecurity in the US and EU.

Conducting this comparison will serve for insights to, on the one hand, manufacturers and other relevant stakeholders and, on the other hand, policymakers and lawmakers on both sides of the Atlantic about different approaches taken for regulating this matter. Next to outlining their implications, this research evaluates both systems' main strengths and limitations, with the ultimate goal of understanding which system provides more solid protection (at least theoretically) regarding cybersecurity for AI-based medical devices to patients who are the most at risk. By combining these two methods, this White Paper aims to provide recommendations about the main advantages of both systems, their downsides, and feasible normative and policy approaches that could be taken to improve the system that will benefit all stakeholders involved.

Comparative analysis

Cybersecurity of AI-based medical devices requires the assessment of three areas subject to evolving regulatory approaches: medical devices, AI, and cybersecurity. Although they may appear distinguished in regulatory matters, the existence of AI-based medical devices and their possible cyber vulnerabilities makes clear that the three areas are intertwined and deserve closer attention from a regulatory point of

view. For this reason, the following section provides analysis from three angles: applicable legislation, soft law documents, and an overview of the state-of-the-art literature analysis.

The US approach

Legislation

In December 2022, the US President signed a new statute which impacts the regulation of medical device cybersecurity in the US[1]. Namely, Section 3305 of the Consolidated Appropriations Act of 2023 provides authority to the FDA to establish cybersecurity standards for medical devices. In particular, Section 3305 aims to address cybersecurity-related concerns associated with medical devices that the FBI's Cyber Division reported in 2022[2]. It authorizes the FDA to implement and enforce new regulatory standards for premarket submissions of medical devices with the goal of securing devices as soon as they are put on the market. Under this new law, the entity submitting a premarket medical device application (the sponsor) is obliged to comply with the following four obligations if such a medical device is defined as a 'cyber device'[3]. First, the sponsor must submit to the FDA Secretary a plan detailing how it will monitor, identify and address in a reasonable time postmarket cybersecurity

[1] See Consolidated Appropriations Act, 2023, available at: https://www.appropriations.senate.gov/imo/media/doc/JRQ121922.PDF.

[2] The report states that medical devices cybersecurity-related vulnerabilities could significantly impact on patients safety, data confidentiality, data integrity, functioning of healthcare facilities, as well as provoke significant costs for the cyberattacks' victims. See https://www.aha.org/system/files/media/file/2022/09/fbi-pin-tlp-white-unpatched-and-outdated-medical-devices-provide-cyber-attack-opportunities-sept-12-2022.pdf.

[3] 'Cyber device' is a device that includes software that is validated, installed, or authorized by the sponsor, which has the ability to connect to the Internet and it contains any technological characteristics that could be vulnerable to cybersecurity threats.

vulnerabilities. Second, the sponsor is obliged to design, develop, and maintain processes and procedures providing enough assurance that the device is cyber secure and make available postmarket updates to the device to address, on a reasonably justified regular cycle, known unacceptable vulnerabilities and as soon as possible, any critical vulnerabilities that could provoke uncontrolled risks to the device. Third, the sponsor must provide the FDA Secretary with a software bill of materials (including commercial, open source and off-the-shelf software components). And fourth, the sponsor must comply with any other requirements required by the FDA Secretary through regulation in order to demonstrate reasonable assurance that the device is cybersecure. This legislation represents a significant step in recognizing the relevance of medical device cybersecurity in the US since manufacturers of medical devices connected to the Internet must first show them to the FDA and prove that they have a clear vision of how they plan to deal with potential cybersecurity threats.

Soft law

Compared with the EU, the US regulator addressed the issue of medical device cybersecurity. In 2005, the Food and Drug Administration (FDA) agency outlined the general principles for Networked Medical Devices Containing Off-the-Shelf Software that is vulnerable to cybersecurity threats (such as viruses and worms). Already then, the FDA recognized the importance of cybersecurity when medical devices connect to the Internet, which requires ongoing cybersecurity maintenance through the lifecycle of the device in order to ensure an adequate cybersecurity level. This Guidance was followed by the 2014 and 2016 Guidance for Premarket Submission (which is intended to establish effective cybersecurity management to reduce risks to patients caused by

cybersecurity risks) and Postmarket Management of Cybersecurity in Medical Devices (which provides recommendations for managing postmarket cybersecurity vulnerabilities for marketed and distributed medical devices). In addition to these, there exist two pieces of Draft Guidance, not final yet: the 2018 Content of Premarket Submissions for Management of Cybersecurity in Medical Devices and the 2022 Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submission, which is expected to replace the 2018 draft guidance. Concerning AI medical devices, the FDA traditionally reviews medical devices through premarket pathways such as premarket clearance (510(k)), De Novo classification or premarket approval.

Literature

Medical device law is a *niche* field recently attracting legal scholars' attention in the US (Eskenazy, 2016). Academic contributions concerning US regulations have focused on different legal aspects of medical device cybersecurity. Many authors have observed the statutory and regulatory gaps in US legislation concerning medical device cybersecurity (see, e.g. Hagen, 2016; see also Kersbergen, 2017, on patient privacy and safety; Tschider, 2017, on the insufficiency of the statutory framework in reducing cybersecurity risks). Some scholars even compared the US framework with the EU one from the cybersecurity perspective (Lyapustina & Armstrong, 2018), (Skierka, 2018) or with reference to cybersecurity requirements (Chen et al., 2018). In some cases, medical device cybersecurity is tackled only as an issue of a broader topic (see, e.g. Cohen et al., 2020) or within a more general discussion on health cybersecurity (C. A. Tschider, 2017). Other authors commented on specific kinds of medical devices, such

as implantable medical devices (Browning & Tuma, 2016) or cardiac defibrillators cybersecurity (Woods, 2017).

The doctrine also commented on the link between medical device cybersecurity and critical infrastructure protection (Check, 2023); best practices for the regulation of medical device cybersecurity (Shackelford et al., 2018) or metrics for assessing the security of implantable medical devices (Camara et al., 2015). Lord and Dillon (2019) described the problem of legacy devices (Lord & Dillon, 2019); Johnson proposed a safe harbour for them (Johnson, 2022). Liability, in general, is an aspect that has been explored for some years. In 2014, Wellington illustrated the difficulties of identifying and deterring the malicious actors behind cyberattacks. (Wellington, 2014). In 2017, Dudin approached this issue from a tort law perspective (Dudin, 2017), followed by Montesantos (2022) and Corbin (2019). Other pieces of the literature underscored the limits of the existing workforce for medical device cybersecurity (Lord & Dillon, 2019).

Notwithstanding its overall maturity, the doctrinal discussion on medical device cybersecurity has failed to comment on the regulatory aspects concerning the cybersecurity of AI-based medical devices. Only after 2018, the debates held at the FDA level concerning Software as a Medical Device (SaMD) led many scholars to dedicate their attention to AI-based medical device regulation. (e.g. (Babic et al., 2019; Gilbert et al., 2021), but not many yet on AI-based medical device cybersecurity. Tschider is one of the few authors that did it. Tschider's work represents a pioneering and fundamental piece of research advancing the AI-based medical device cybersecurity regulation debate. In 2018, her *Regulating Cybersecurity and Artificial Intelligence* explained specific areas of concern for patient safety and evaluated the new technology gaps in the EU and US regulatory frameworks (C. A. Tschider, 2018).

Tschider noted the lack of developed models considering AI impacts on medical device cybersecurity. The article was followed by another one in 2021 on AI-based medical devices from a tort law perspective (A. Tschider, 2021). However, to this date, the article is unfortunately no longer updated to the most recent developments concerning the FDA's advancements in AI/ML SaMD regulation. An interesting follow-up by Boubker (2021) included notes on AI-based medical devices and stated that the FDA guidance is insufficiently tackling AI-based medical device cybersecurity (Boubker, 2021). Nevertheless, the paper focused not only on medical device cybersecurity, and the arguments would require further expansion. In conclusion, the literature often recognizes the cybersecurity of medical devices as of core importance. However, little attention to AI-related aspects shows the existing gaps that would need to be filled by scholarly contributions.

The EU approach

Legislation

Medical devices' cybersecurity is regulated at the EU level through sector-specific legislation that simultaneously applies to all the EU Member States: the Medical Device Regulation (MDR). The MDR includes cybersecurity provisions in its Annex I, containing several safety requirements (Biasin & Kamenjasevic, 2022a). Article 5(1) MDR obliges manufacturers to ensure that the device complies with the MDR obligations when used according to its intended purpose. According to Article 5(2) MDR, a medical device shall meet the general safety and performance requirements set out in Annex I MDR, taking into account the intended purpose. As part of the general requirements set in Annex I MDR, medical devices shall achieve the performance intended by the manufacturer (MDR, Annex I, req 1) and be designed in a way suitable for the intended use. They shall be safe and effective, and associated risks shall be acceptable when weighed against the benefits of the patients and the level of protection of health and safety while taking into account state of the art. Moreover, manufacturers shall establish, implement, document, and maintain a risk management system, including risk control measures to be adopted by manufacturers to design and manufacture a device that conforms to safety principles and state-of-the-art (MDR, Annex I, req 4). A medical device designed to be used with other devices/equipment as a whole (including the connection system between them) has to be safe and should not impair the specified performance of the device. Furthermore, a medical device shall be designed and manufactured to remove, as far as possible, risks associated with possible

negative interaction between software and the IT environment within which they operate. If a medical device is intended to be used with another device, it shall be designed so that interoperability and compatibility are reliable and safe (MDR, Annex I, req 14). A medical device incorporating electronic programmable systems, including software or standalone software as a medical device, must be designed to ensure repeatability, reliability, and performance according to the intended use, and appropriate means have to be adopted to reduce risks or impairment of the performance. A medical device should be developed and manufactured according to the state-of-the-art and by respecting the development life cycle principles, risk management (including information security), verification, and validation. Finally, manufacturers must set out minimum requirements concerning hardware, IT network characteristics, and IT security measures, including protection against unauthorized access (MDR, Annex I, req 17). Concerning information to be supplied together with the device, manufacturers must inform about residual risks, provide warnings requiring immediate attention on the label and, for electronic programmable system devices, give information about minimum requirements concerning hardware, IT networks' characteristics and IT security measures (including protection against unauthorized access), necessary to run the software as intended (MDR, Annex I, req 23). In addition to the MDR, other existing and forthcoming pieces of legislation are relevant for AI-based medical device cybersecurity. The NIS2 Directive broadens its scope of application with a significant impact on the healthcare sector. Healthcare providers (already included in the NIS Directive as OES) remain in the scope of the legislation, and now they are considered 'essential entities' (Annex I). In addition to these, the NIS2 Directive adds new types of entities relevant to the healthcare sector. Under 'essential entities', the Directive now includes EU reference laboratories, entities

carrying out R&D activities of medicinal products, entities manufacturing basic pharmaceutical products and preparations, and manufacturers of medical devices considered critical during a public health emergency. Concerning 'important entities', the Directive includes the 'entities manufacturing medical devices and in vitro diagnostic medical devices' (see Annex II NIS2 Directive proposal). Since these categories are not included in the NIS Directive, it represents a core change for the medical devices sector. Similarly to the NIS Directive, the NIS2 Directive mandates the Member States to establish a set of security measures for the entities under its personal scope. Chapter IV of the Directive contains cybersecurity, risk management, and reporting obligations. Article 18 of the proposal on cybersecurity risk management measures implies that essential and important entities shall take appropriate and proportionate technical and organizational measures to manage the risks posed to the security of network and information systems. Article 20 of the Directive on reporting obligations introduces a two-step procedure to report significant security breaches, which could also be reported to the recipients of their services. Article 21 of the Directive concerns cybersecurity certification schemes. Enforcement and supervision of essential and important entities are delegated to competent authorities. Competent authorities shall supervise them and ensure their compliance with the security and incident notification requirements. An *ex-ante* supervisory regime is in place for essential entities and an *ex-post* one for important entities.

The AI Act proposal will be relevant regarding medical devices incorporating or being AI systems (Biasin & Kamenjasevic, 2022b). Under Article 6 (1)(b) and Annex II (section 11) of the AI Act proposal, most medical devices classify as high-risk AI systems. Consequently, the following recitals and provisions of the AI Act proposal would be applicable to their providers when it comes to implementing cybersecurity

requirements. Recital 51 acknowledges cybersecurity's role in ensuring AI systems' resilience against cyberattacks attempting to alter their use, behaviour, performance, or compromise their security properties. Providers need to take suitable measures to ensure an appropriate level of cybersecurity for high-risk AI systems. Further on, Recital 43 of the proposal refers to the requirements that high-risk AI systems should respect in order to effectively mitigate the risks for health, safety and fundamental rights, as applicable in the light of the intended purpose of the system, and no other less trade-restrictive measures are reasonably available, thus avoiding unjustified restrictions to trade. One of these requirements is cybersecurity. In that regard, Recital 49 states that high-risk AI systems need to perform consistently throughout their lifecycle and meet an appropriate level of cybersecurity in accordance with state-of-the-art. Article 13(1) of the proposal requires that high-risk AI systems are designed and developed to ensure their transparent operation so the users can interpret the system's output and use it appropriately. In the instructions for use (Article 15(2-3)), providers shall specify the level against which cybersecurity of the system has been tested and validated, which can be expected and any known and foreseeable circumstances that may impact that level of cybersecurity. Article 15(4) of the proposal requires that the technical solutions aimed at ensuring the cybersecurity of high-risk AI systems are appropriate to the relevant circumstances and the risks. To this end, high-risk AI systems certified according to Article 56 of the EU Cybersecurity Act shall be presumed to comply with the cybersecurity requirements set out in the proposal (AI Act proposal, Article 42).

Soft law

The Medical Device Coordination Group (MDCG) issued the first EU-wide guidance on the Cybersecurity of Medical Devices (Medical Device Coordination Group, 2019) in December 2019. The Guidance illustrates the most relevant safety requirements relevant to cybersecurity as applied to medical devices. The Guidance provides a comprehensive overview of cybersecurity-related requirements that manufacturers must implement to comply with the MDR and ensure the medical device's appropriate level of cyber resilience. Moreover, the Guidance highlights that ensuring the cybersecurity of medical devices is a joint responsibility, including manufacturers, suppliers, healthcare providers, patients, integrators, operators, and regulators. For example, manufacturers are bound by the majority of the provisions mentioned in the MDR. Integrators are, among other obligations, responsible for assessing a reasonable level of security. Operators need to ensure the required level of security for the operational environment and that personnel is appropriately trained on cybersecurity issues. Healthcare professionals are responsible for using a device according to its intended use, while patients and consumers need to "employ cyber-smart behaviour." The meaning of "cyber-smart behaviour" remains unclear. The word is not present in EU regulations or soft law, but some inspiration may be taken from the Australian Government Department of Home Affairs' Action Plan. These stakeholders are an equally important part of the cybersecurity chain (Kamenjasevic, 2018), and each stakeholder is responsible for ensuring a secure environment in which a device can smoothly operate for the ultimate benefit of patients' safety (MDCG, 2019; IMDRF, 2019).

Literature

The literature state-of-the-art concerning medical device cybersecurity regulation is similar, to some extent, to the one existing in the US. In the EU, however, the majority of studies focused on the topic of medical device cybersecurity regulation only in recent years. Our literature review found different kinds of approaches towards the matter. Some authors, for example, approach medical device cybersecurity regulation from broader perspectives – such as medical IoT (Chiara, 2022) – specific devices – such as robots (Fosch-Villaronga & Mahler, 2021; Giansanti & Gulino, 2021) or ingestible electronic sensors (Gerke et al., 2019) – or fields of application – including radiology (Pesapane et al., 2018).

Many contributions offer a technical perspective with some regulatory or legislative remarks. Our analysis is not exhaustive in that regard since we focused on legal scholarship, but we could mention some examples. Granlund and others (2021) analyzed the MDCG guidance on the cybersecurity of medical devices from a technical perspective (Granlund et al., 2021); some contributions have illustrated the relevance of certain requirements and standards to medical device cybersecurity (Lechner, 2017; Ravizza et al., 2019; Sadhu et al., 2022), in some cases bringing specific case studies (Taylor et al., 2022). Others offered views on the role of education for engineers for cybersecurity legal requirements (Lhotska, 2021) or commented on the role of transparency for cybersecurity in medical writings (Billiones, 2017).

From the perspective of strictly legal scholarship, there are fewer contributions if compared to the US. Many retain themselves to descriptive work (Tasheva & Kunkel, 2022). Others engage in comparative perspectives (Calcagnini et al., 2022; Yeng et al., 2020), sometimes coupled with an issue-specific comparison (Skierka, 2018). There is a strand analyzing the effects of cybersecurity from the lens of liability (Ludvigsen &

Nagaraja, 2022). Another strand analyses the issue of cybersecurity regulation for medical devices regarding the interplay between the different existing or forthcoming legislation in the EU (Biasin & Kamenjasevic, 2022; Biasin & Kamenjašević, 2022). Finally, the recent debates on AI regulation led many scholars to dedicate their attention to AI medical device regulation (Gerybaite et al., 2022; Kiseleva, 2020). Some contributions in the literature touch upon medical device software using AI and mention cybersecurity – but not with an in-depth analysis of the latter (Ahmad et al., 2020; Gerke et al., 2020; Grzybowski & Brona, 2023; Mahler et al., 2021; Minssen, Gerke, et al., 2020; Mkwashi, Andrew & Brass, Irina, 2022). A recent contribution is devoted explicitly to AI-based medical device cybersecurity regulation (Biasin et al., 2023), but it does not insist on EU/US comparative remarks. Therefore, one could conclude that in the case of EU scholarship, there are gaps in the literature concerning the cybersecurity of AI-based medical devices that need to be filled by scholarly contributions.

Discussion

The two systems into perspective – The literature on the EU-US comparison has focused on several issues, including liability, transparency and vulnerability reporting for cyber attacks on medical devices, the responsibility of regulatory bodies, and others. These studies focused on medical device cybersecurity without focusing (except for some liability studies) on the AI-based aspects. Nevertheless, AI regulation brings new aspects worth comparing the EU and US legal systems to add to the overall analysis. Our analysis focused on three different areas. The first area is legislation, where we compare the state-of-the-art in the EU and US for the laws concerning AI-based medical devices. The second area is regulation. By regulation, we mean all the aspects surrounding the regulatory Guidance and orientations that competent health authorities could issue about AI-based medical device cybersecurity. The third area we investigate is the scope of legislation for medical devices. There, we identify the possible differences that the definition of medical devices could entail in terms of scope and, thus, application of cybersecurity-related requirements for AI-based medical devices. The table below summarises our findings, further explained in the following sections.

	US	EU
Legislation	**Existence of relevant laws.** At the federal level: ▪ legislation on MD ▪ laws on cybersecurity ▪ no federal laws on AI (only state-specific)	**Existence of relevant laws.** At the EU level, ▪ legislation on MD ▪ laws on cybersecurity ▪ laws on AI
Regulation	**Existing Guidance** ▪ Cybersecurity guidance ("may apply to AI-based medical devices"). ▪ AI: AI/ML Good practices (refer to cybersecurity)	**Existing Guidance** ▪ Cybersecurity: Guidance (no reference to AI) ▪ AI: no guidance
Scope	**Problematic definition** ▪ Too narrow: The definition of medical devices excludes several AI-based health products.	**Problematic definition** ▪ Possible loopholes: The definition of medical leaves interpretative room for excluding certain low-risk devices. ▪ Too narrow: the proposed AI Act excludes certain low-risk medical from its additional rules on cybersecurity.

Table 1: EU/US systems on AI-based medical device cybersecurity

Legislation

Laws on AI, cybersecurity and medical devices – Before analyzing AI-based medical device cybersecurity, it is essential to consider the law of medical devices, AI *and* cybersecurity and see how they interrelate. The EU has distinct and concurring regulations for AI-based medical devices. Let us start with medical device laws. Although they do not explicitly mention "AI" and "cybersecurity", they are relevant to AI-based medical devices for their rules on medical device software. The second category is AI law. The EU is adopting a new, cross-sectoral regulation concerning AI (the AI Act), which includes cybersecurity-related requirements applicable to AI-based high-risk medical devices. The third category is cybersecurity laws. These include the NIS 2 Directive, which imposes cybersecurity requirements for medical device manufacturers. Section 2 shows these three categories of laws apply concurrently and have distinct cybersecurity-related requirements to consider.

In the US, the primary legislation to consider for medical device laws is the Food, Drug, and Cosmetics Act (FD&C Act). The FD&C Act, however, does not refer to "AI", although its requirements on software as a medical device could be related to the legal text. Unlike the MDR, the FD&C Act explicitly refers to cybersecurity (under section §360n–2 titled "Ensuring cybersecurity of devices") and foresees specific requirements. Turning now to AI Laws, in the US, no comprehensive federal law legislation is solely dedicated to AI. Existing laws, such as on data privacy or non-discrimination, touch upon certain AI aspects.[4] Finally, general cybersecurity laws,

[4] In healthcare, some AI-related bills are currently under discussions. See Epic.org (2023) website for a list.("The State of State AI Laws," 2023). These laws are primarily concerned with mental health

such as the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), foresee incident reporting and other requirements soon to be specified by forthcoming comprehensive guidelines on reporting.

Comparative remarks – The comparison of the current state of the art in the EU/US legislation on AI-based medical device cybersecurity reveals the different situations where the two legal systems stand. The shared point of both legal systems resides in having ad hoc medical device laws in place. Both medical device laws contain relevant requirements from a cybersecurity point of view. AI-related requirements, however, are not explicit, and these are to be inferred from specific rules – such as those on medical device software (EU) or SaMD (US). Similarly, safety is the broader category, including cybersecurity-related requirements.[5] Turning to AI legislation, AI-specific legislation exists at the EU level, whereas in the US (to date), there is no federal law on AI. For cybersecurity laws, both the EU and the US have their laws in place. All of them must interrelate with AI and medical device legislation, including for their cybersecurity-related requirements.

In light of this legislative setting, the question that may arise is whether all these legal instruments come together harmonically. In a previous EU-focused study on AI-based medical device cybersecurity legislation, we found that the EU legislator failed to adopt a holistic approach to regulating medical device cybersecurity (Biasin, Yasar, Kamenjasevic, *forthcoming,* 2023). More specifically, in our paper with Yaşar, we found that new regulations on data and AI – introducing new cybersecurity

autonomy and the intervention of a healthcare professional in automated decision making or discrimination

[5] In its guidance, the FDA (2023; p. 5) specifies that "Cybersecurity is Part of Device Safety and the Quality System Regulation".

requirements for medical devices – are not aligned with the existing cybersecurity laws and their requirements (Biasin et al, *forthcoming,* 2023).

Turning the attention to the US legal system, the studies we found in our literature review have treated and compared, to some extent, the interplay between some pieces of legislation (e.g. the HIIPA) with medical devices for cybersecurity. However, given the recent approval of the CIRCIA, more insights might be needed to understand whether the existing requirements are coming together coherently. To our knowledge, there is still little focus on applying the CIRCIA law to medical device cybersecurity legislation.[6] We think, therefore, that further research in this respect is desirable, especially to ascertain how the different requirements will come into place.

Regulation

Regulatory Guidance on cybersecurity of AI-based medical devices – We now analyze the current state-of-the-art available Guidance on AI-based medical device cybersecurity by considering the documents dedicated to cybersecurity and artificial intelligence. In the EU, there is no AI-specific guidance for medical devices. The most relevant piece of guidance is on medical device software. In this guidance, no reference is made to AI. The same guidance references cybersecurity (Medical Device Coordination Group, 2020, p. 13). In 2019, the plans of the MDCG included a possible report on AI medical devices – which, to date, is no longer in their plans. Moving our attention to cybersecurity regulation, the MDCG – as seen above – has already issued Guidance on the cybersecurity of medical devices. However, such guidance does not mention "AI" nor exemplify the possible risks and aspects that could affect them. The

[6] The most relevant piece of comparison the US and the EU legislation on cybersecurity is by Bearwood (Beardwood, 2023). The piece, however, does not focus on healthcare.

cybersecurity guidance was drafted in late 2019, and AI was probably not a core concern back then. In our view, it would be necessary that MDCG updates or issues new Guidance tackling the AI-related aspects of medical device cybersecurity.

In the US, the FDA has been significantly more active in producing cybersecurity-related Guidance. In the last years, the FDA has produced numerous pieces of Guidance.[7] Moreover, it has also been particularly proactive regarding artificial intelligence and its possible regulatory pathways. Furthermore, in its Good Machine Learning Practices for Medical Device Development, the FDA included the implementation of "good software engineering and security practices", including robust cybersecurity practices.

Comparative remarks – The description of the US and EU situation illustrates the different pace at which the US regulatory authority stands if compared with the EU. At this moment, probably because the MDCG is waiting for the approval of the AI Act in the EU, there is a general lack of attention to any AI-related aspect of medical devices, including medical device cybersecurity.[8] The US FDA, on the contrary, is a prolific actor in terms of issuing cybersecurity guidance with relevance to AI-based medical device cybersecurity. Such cybersecurity risks could ultimately originate from AI-related issues and thus be relevant for AI-based medical devices.

[7] As an example, the latest FDA guidance specifies that the security objectives of medical device designing for security may apply to devices containing artificial intelligence and machine learning (FDA, 2023; p. 7).

[8] Nevertheless and in addition to the remarks above, it is crucial to report the existence of the supranational orientations produced by the International Medical Device Regulators Forum (IMDRF), which has produced guidance on medical device software/SaMD, medical device cybersecurity, and AI/ML-related aspects of medical devices. The EU and the US are part of this regulatory forum, so they will have to adhere to them.

Scope and definitions

Medical Devices – The third area of analysis concerns the application of the laws and regulatory Guidance assessed in the former sections. That third analysis is because the scope of the said laws and guidance documentation passes through the definition of medical devices. In the EU, medical device laws apply to the medical devices defined in MDR article 2.[9] The definition in medical device law has entailed some interpretative issues, which the literature has been reporting about for some years (Ludvigsen et al., 2022; Mantovani & Bocos, 2017).[10] The literature has historically criticized the definition of medical devices because it delegates the manufacturers to determine whether devices are low-risk medical devices or wellness applications (Ludvigsen et al., 2022; Mantovani & Bocos, 2017; Minssen, Mimler, et al., 2020). Such a factual situation implies that software that could fall under the 'low risk' is in a loophole for manufacturers to escape stricter medical device laws. This problem becomes relevant for AI-based medical device cybersecurity: AI-based software falling outside this definition of medical device implies manufacturers will not have to comply with cybersecurity-related requirements established by the MDR. To this issue, there is more to add. As seen above, the forthcoming AI Act will also apply to medical devices. However, the application of the AI Act is subordinated to the medical devices'

[9] In the EU, medical devices are defined under article 2 as "'medical device' means any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes: — diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease, — diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability, — investigation, replacement or modification of the anatomy or of a physiological or pathological process or state, — providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations, and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means."

[10] More specifically, the definitory problem of medical devices is inherently connected with the notion of intention/ intended purpose.

definition in the MDR and their risk classification.[11] Only if medical devices are of high-risk classes according to the MDR/IVDR will the AI Act requirements (including the cybersecurity ones) apply.[12] As Palmieri and Goffin commented, this choice may however fall short of protecting individuals' safety and fundamental rights. This because apps and health AI software qualifying as low risk medical devices could still bring considerable risks for patients (Palmieri & Goffin, 2023).

On the US side, the definition of medical devices is provided by section 201(h)(1) of the F&DCA.[13] Similarly to the EU case, the technology falling under the definition of a medical device must comply with medical device law's cybersecurity rules. Also, in the US, there are open questions concerning the definition of medical devices. More specifically, certain scholars criticized the definition of medical devices for being too narrow and not including several risky AI-based health products (Gerke, 2021). The same author also noted that the definition does not encompass Clinical Decision Support (CDS) software, AI-based mortality prediction models, and other models that are intended for use in the prediction or prognosis of disease or other conditions –

[11] Some authors (Palmieri & Goffin, 2023) have proposed schematic presentation of the interplay between the AI Act and other relevant regulations to understand the interplay of the MDR and AI Act. First, one should evaluate whether the software in consideration is to be considered as an AI system, according to the AI Act. Outside the definition of AI system, the medical device software will not entail the use of AI and therefore, although it remains software, it will be excluded from AI-related evaluations.

[12] The AI Act (in its Article 6) establishes that AI systems falling under the MDR/IVDR that must undergo a third-party conformity assessment shall be considered high risk

[13] The article defines medical devices as: "an instrument, apparatus, implement, machine, contrivance implant, in vitro reagent, or other similar or related article, including any component, part, or accessory, which is— (A) recognised in the official National Formulary, or the United States Pharmacopeia, or any supplement to them, (B) intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or (C) intended to affect the structure or any function of the body of man or other animals, and which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolised for the achievement of its primary intended purposes. The term "device" does not include software functions excluded pursuant to section 520(o)".

which should, in turn, be considered as medical devices to ensure a higher level of safety of these technologies (id.; p. 511).

Comparative remarks – Although for different reasons, many scholars in the EU and US academia seem to agree that, when it comes to AI-based medical devices, the existing definitions are problematic and potentially risk bringing safety risks for patients. For different reasons, the US and the EU have narrow definitions, excluding certain kinds of medical devices from the scope of application of the relevant legislation (the FD&C Act for the US and the AI Act proposal for the EU). Furthermore, in the EU, the issue is exacerbated by the long-known problem of the 'intention/intended purpose', which can potentially exclude specific low-risk medical devices from the medical device's stricter legal regime.[14] In conclusion, such exclusions may be problematic for ensuring a higher level of safety for end users and patients, which ultimately could be using AI-based health technologies that – in principle – could or should qualify as medical devices.

Conclusions and recommendations

- The field focusing on AI-based medical device cybersecurity is relatively new and still in the process of being established in the US and EU.
- **Literature** is blooming, but it is still relatively scarce. Legal literature and its comparative analyses could help identify and address specific problems. Many open questions need to be discussed and analyzed, such as:

[14] Finally, in its analysis, Gerke observes that the regulation of medical devices should consider them also as systems, not just devices (Gerke, 2023; p. 504). Although with discussed limitations, this problem seems to be tackled in the EU, as the AI Act is focused on AI systems

  - Medical device software and the implications of their possible loopholes in the EU/US definitions in relation to AI cybersecurity;
  - AI-based related aspects of medical device cybersecurity, such as the threats and the legal aspects addressing them.

- **EU laws** are in the making. More and more legislation refers to cybersecurity and considers it essential to products and services. At the same time, gaps and overlaps between them remain to be addressed. For example, the AI Act proposal should be used as an opportunity for the EU legislators to tackle this issue in more depth (despite having a different focus).
- **US laws** are in the making, too. The interplay between broader cybersecurity laws (such as the CIRCIA) and specific cybersecurity requirements foreseen in medical device laws must be further explored.
- **Soft laws** are an important tool and should be further exploited as a means to provide Guidance concerning specific issues that cannot be extensively addressed with the legislation itself. In the EU, there is a lack of such guidance provided for manufacturers. The US leads with good examples in this regard. In the broader context, the US and the EU may consider the existing orientations agreed by the IMDRF, which has issued guidelines regarding AI and cybersecurity.
- **Regulatory oversight** also remains a crucial element that presents differences within both legal systems. The US centralized governmental system makes it more likely that authorities have a stronger grip on the oversight of medical devices' safety requirements since they can monitor them continuously and throughout their lifecycle. This grip might be less effective in the EU, as it

relies on a third-party notification system assessment while leaving the postmarket checks to the Member States' regulatory authorities.

- The EU and the US lack **standards** for AI-based medical device cybersecurity. Ultimately, such standards and best practices would be highly desirable for manufacturers – in achieving and demonstrating compliance – and for regulatory authorities to assess the devices from the pre- to postmarket phase.

Bibliography:

Ahmad, O. F., Stoyanov, D., & Lovat, L. B. (2020). Barriers and pitfalls for artificial intelligence in gastroenterology: Ethical and regulatory issues. Techniques and Innovations in Gastrointestinal Endoscopy, 22(2), 80–84. https://doi.org/10.1016/j.tgie.2019.150636

Babic, B., Gerke, S., Evgeniou, T., & Cohen, I. G. (2019). Algorithms on regulatory lockdown in medicine. Science, 366(6470), 1202–1204. https://doi.org/10.1126/science.aay9547

Biasin, E., & Kamenjasevic, E. (2020). Cybersecurity of medical devices. Regulatory challenges in the EU. SSRN Electronic Journal. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3855491

Biasin, E., & Kamenjašević, E. (2022). Cybersecurity of medical devices: New challenges arising from the AI Act and NIS 2 Directive proposals. International Cybersecurity Law Review, 3(1), 163–180. https://doi.org/10.1365/s43439-022-00054-x

Biasin, E., & Kamenjasevic, E. (2022a). 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). Cambridge: Cambridge University Press. doi:10.1017/9781108975452.005

Biasin, E., Kamenjasevic, E., Ludvigsen, K. R., Solaiman, B., & Cohen, I. G. (2023). Cybersecurity of AI medical devices: Risks, legislation, and challenges. Edward Elgar. https://doi.org/10.48550/arXiv.2303.03140

Biasin, E., Yasar, B., Kamenjasevic, E. (*forthcoming, 2023).* New Cybersecurity Requirements for Medical Devices in the EU: The Forthcoming European Health Data Space, Data Act and Artificial Intelligence Act. Law, Technology and Humans, 5(2).

Billiones, R. (2017). Medical devices in the disclosure era and the role of medical writers. Medical Writing, 26(2), 32–34.

Boubker, J. (2021). When Medical Devices Have a Mind of Their Own: The Challenges of Regulating Artificial Intelligence. American Journal of Law & Medicine, 47(4), 427–454. https://doi.org/10.1017/amj.2022.3

Browning, J. G., & Tuma, S. (2016). If Your Heart Skips a Beat, It May Have Been Hacked: Cybersecurity Concerns with Implanted Medical Devices. South Carolina Law Review, 67(3), 637-[1].

Calcagnini, G., Censi, F., & Mattei, E. (2022). Information and Communication Technology: Implications on Patient's Privacy and Security. In C. Boccato, S. Cerutti, & J. Vienken (Eds.), Medical Devices (pp. 129–138). Springer International Publishing. https://doi.org/10.1007/978-3-030-85653-3_7

Camara, C., Peris-Lopez, P., & Tapiador, J. E. (2015). Security and privacy issues in implantable medical devices: A comprehensive survey. Journal of Biomedical Informatics, 55, 272–289. https://doi.org/10.1016/j.jbi.2015.04.007

Check, T. (2023). The Tallinn Manual 2.0 on Nation-State Cyber Operations Affecting Critical Infrastructure. American University National Security Law Brief, 13(1).

Chen, Y.-J., Chiou, C.-M., Huang, Y.-W., Tu, P.-W., Lee, Y.-C., & Chien, C.-H. (2018). A Comparative Study of Medical Device Regulations: US, Europe, Canada, and Taiwan. Therapeutic Innovation & Regulatory Science, 52(1), 62–69. https://doi.org/10.1177/2168479017716712

Chiara, P. G. (2022). The IoT and the new EU cybersecurity regulatory landscape. International Review of Law, Computers & Technology, 36(2), 118–137. https://doi.org/10.1080/13600869.2022.2060468

Chiara, P. G. (2022). The IoT and the new EU cybersecurity regulatory landscape. International Review of Law, Computers & Technology, 36(2), 118–137. https://doi.org/10.1080/13600869.2022.2060468

Cohen, I. G., Gerke, S., & Kramer, D. B. (2020). Ethical and Legal Implications of Remote Monitoring of Medical Devices. The Milbank Quarterly, 98(4), 1257–1289. https://doi.org/10.1111/1468-0009.12481

Corbin, B. A. (2019). When "things" go wrong: Redefining liability for the Internet of medical things. South Carolina Law Review, 71(1), 1–44.

Dudin, L. (2017). Networked Medical Devices: Finding a Legislative Solution to Guide Healthcare into the Future. Seattle University Law Review, 40(3), 1085.

Eskenazy, D. (2016). Le dispositif médical à la recherche d'un nouveau cadre juridique. https://tel.archives-ouvertes.fr/tel-01461616

FDA. (2020). Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD). https://www.fda.gov/media/122535/download

FDA. (2022). Cybersecurity. FDA. https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity

Fosch-Villaronga, E., & Mahler, T. (2021). Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots. Computer Law & Security Review, 41, 105528. https://doi.org/10.1016/j.clsr.2021.105528

Gerke, S., Minssen, T., & Cohen, G. (2020). Ethical and legal challenges of artificial intelligence-driven healthcare. In Artificial Intelligence in Healthcare (pp. 295–336). Elsevier. https://doi.org/10.1016/B978-0-12-818438-7.00012-5

Gerke, S. (2021). Health AI for Good Rather Than Evil? The Need for a New Regulatory Framework for AI-Based Medical Devices. Yale Journal of Health Policy, Law, and Ethics, 20(2).

Gerybaite, A., Palmieri, S., & Vigna, F. (2022). Equality in Healthcare AI: Did Anyone Mention Data Quality? BioLaw Journal - Rivista Di BioDiritto, 385-409 Paginazione. https://doi.org/10.15168/2284-4503-2483

Giansanti, D., & Gulino, R. A. (2021). The Cybersecurity and the Care Robots: A Viewpoint on the Open Problems and the Perspectives. Healthcare, 9(12), 1653. https://doi.org/10.3390/healthcare9121653

Gilbert, S., Fenech, M., Hirsch, M., Upadhyay, S., Biasiucci, A., & Starlinger, J. (2021). Algorithm Change Protocols in the Regulation of Adaptive Machine Learning–Based Medical Devices. Journal of Medical Internet Research, 23(10), e30545. https://doi.org/10.2196/30545

Granlund, T., Vedenpaa, J., Stirbu, V., & Mikkonen, T. (2021). On Medical Device Cybersecurity Compliance in EU. 2021 IEEE/ACM 3rd International Workshop on Software Engineering for Healthcare (SEH), 20–23. https://doi.org/10.1109/SEH52539.2021.00011

Grzybowski, A., & Brona, P. (2023). Approval and Certification of Ophthalmic AI Devices in the European Union. Ophthalmology and Therapy, 12(2), 633–638. https://doi.org/10.1007/s40123-023-00652-w

Hagen, L. (2016). Coding for Health: Cybersecurity in Medical Devices. Health Lawyer, 28(5).
Johnson, A. (2022). Closing the Cybersecurity Gap in Medical Devices—Proposing a Safe Harbor System. Colorado Technology Law Journal, 20(1), 161–176.

Kersbergen, C. (2017). PATIENT SAFETY SHOULD INCLUDE PATIENT PRIVACY: THE SHORTCOMINGS OF THE FDA's RECENT DRAFT GUIDANCE REGARDING CYBERSECURITY OF MEDICAL DEVICES. Nova Law Review, 41(41), 397–418.

Kestemont, L. (2018). Handbook on Legal Methodology: From Objective to Method. Intersentia; Cambridge Core. https://doi.org/10.1017/9781839702389

Kiseleva, A. (2020). AI as a Medical Device: Is it Enough to Ensure Performance Transparency and Accountability? European Pharmaceutical Law Review, 4(1), 5–16. https://doi.org/10.21552/eplr/2020/1/4

Lechner, N. H. (2017). An overview of cybersecurity regulations and standards for medical device software. Proceedings of the Central European Conference on Information and Intelligent Systems, 237–249.

Lhotska, L. (2021). Role of Legal Issues in Education of Biomedical Informatics. 2021 30th Annual Conference of the European Association for Education in Electrical and Information Engineering (EAEEIE), 1–5. https://doi.org/10.1109/EAEEIE50507.2021.9530745

Lord, R., & Dillon. (2019). Do No Harm 2.0.

Ludvigsen, K. R., & Nagaraja, S. (2022). Dissecting liabilities in adversarial surgical robot failures: A national (Danish) and EU law perspective. Computer Law & Security Review, 44, 105656. https://doi.org/10.1016/j.clsr.2022.105656

Ludvigsen, K. R., Nagaraja, S., & Daly, A. (2022). When Is Software a Medical Device? Understanding and Determining the "Intention" and Requirements for Software as a Medical Device in European Union Law. European Journal of Risk Regulation, 13(1), 78–93. https://doi.org/10.1017/err.2021.45

Lyapustina, S., & Armstrong, K. (2018). Regulatory considerations for cybersecurity and data privacy in digital health and medical applications and products.

Mahler, M., Auza, C., Albesa, R., Melus, C., & Wu, J. A. (2021). Regulatory aspects of artificial intelligence and machine learning-enabled software as medical devices (SaMD). In Precision Medicine and Artificial Intelligence (pp. 237–265). Elsevier. https://doi.org/10.1016/B978-0-12-820239-5.00010-3

Mantovani, E., & Bocos, P. C. (2017). Are mHealth Apps Safe? The Intended Purpose Rule, Its Shortcomings and the Regulatory Options Under the EU Medical Device Framework. In H. R. Marston, S. Freeman, & C. Musselwhite (Eds.), Mobile e-Health. Springer International Publishing.

Medical Device Coordination Group. (2019). MDCG 2019-16 Guidance on Cybersecurity for medical devices. https://health.ec.europa.eu/system/files/2022-01/md_cybersecurity_en.pdf

Mehran Mozaffari-Kermani and others, 'Systematic Poisoning Attacks on and Defenses for Machine Learning in Healthcare' (2015) 19 IEEE Journal of Biomedical and Health Informatics 1893

Minssen, T., Gerke, S., Aboy, M., Price, N., & Cohen, G. (2020). Regulatory responses to medical machine learning. Journal of Law and the Biosciences, lsaa002. https://doi.org/10.1093/jlb/lsaa002

Minssen, T., Mimler, M., & Mak, V. (2020). When Does Stand-Alone Software Qualify as a Medical Device in the European Union?—The Cjeu's Decision in Snitem and What it Implies for the Next Generation of Medical Devices. Medical Law Review, 28(3), 615–624. https://doi.org/10.1093/medlaw/fwaa012

Mkwashi, Andrew, & Brass, Irina. (2022). The Future of Medical Device Regulation and Standards: Dealing with Critical Challenges for Connected, Intelligent Medical Devices. Zenodo. https://doi.org/10.5281/ZENODO.7054049

National Audit Office, UK Deparment of Health. (2018). Investigation: WannaCry cyber attack and the NHS. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf

Palmieri, S., & Goffin, T. (2023). A Blanket That Leaves the Feet Cold: Exploring the AI Act Safety Framework for Medical AI. European Journal of Health Law, 30(4), 406–427. https://doi.org/10.1163/15718093-bja10104

Pesapane, F., Volonté, C., Codari, M., & Sardanelli, F. (2018). Artificial intelligence as a medical device in radiology: Ethical and regulatory issues in Europe and the United States. Insights into Imaging, 9(5), 745–753. https://doi.org/10.1007/s13244-018-0645-y

Ralston, W. (2020, November 11). The untold story of a cyberattack, a hospital and a dying woman. https://www.wired.co.uk/article/ransomware-hospital-death-germany

Ralston, W. (2020, November 11). The untold story of a cyberattack, a hospital and a dying woman. https://www.wired.co.uk/article/ransomware-hospital-death-germany

Ravizza, A., De Maria, C., Di Pietro, L., Sternini, F., Audenino, A. L., & Bignardi, C. (2019). Comprehensive Review on Current and Future Regulatory Requirements on Wearable Sensors in Preclinical and Clinical Testing. Frontiers in Bioengineering and Biotechnology, 7, 313. https://doi.org/10.3389/fbioe.2019.00313

Sadhu, P. K., Yanambaka, V. P., Abdelgawad, A., & Yelamarthi, K. (2022). Prospect of Internet of Medical Things: A Review on Security Requirements and Solutions. Sensors, 22(15), 5517. https://doi.org/10.3390/s22155517

Shackelford, S. J., Mattioli, M., Myers, S., Brady, A., Wang, Y., & Wong, S. (2018). Securing the Internet of Healthcare. Minnesota Journal of Law, Science and Technology, 19(2), 405–454.

Skierka, I. M. (2018). The governance of safety and security risks in connected healthcare. Living in the Internet of Things: Cybersecurity of the IoT - 2018, 2 (12 pp.)-2 (12 pp.). https://doi.org/10.1049/cp.2018.0002

Tasheva, I., & Kunkel, I. (2022). In a hyperconnected world, is the EU cybersecurity framework connected? European View, 21(2), 186–195. https://doi.org/10.1177/17816858221136106

Taylor, K., Smith, A., Zimmel, A., Alcantara, K., & Wang, Y. (2022). Medical Device Security Regulations and Assessment Case Studies. 2022 IEEE 19th International Conference on Mobile Ad Hoc and Smart Systems (MASS), 742–747. https://doi.org/10.1109/MASS56207.2022.00116

Tschider, A. (2021). Medical Device Artificial Intelligence: The New Tort Frontier. Brigham Young University Law Review, 46(6), 1551–1618.

Tschider, C. A. (2017). Enhancing Cybersecurity for the Digital Health Marketplace. Annal Health Law, 26(1), 1.

Tschider, C. A. (2018). Deus Ex Machina: Regulating Cybersecurity and Artificial Intelligence for Patients of the Future. Savannah Law Review, 5, 35.

Wellington, K. B. (2014). Cyberattacks on Medical devices and Hospital Networks: Legal Gaps and Regulatory Solutions. Santa Clara High Technology Law Journal, 30(2), 139-[1].

Woods, M. (2017). Cardiac Defibrillators Need to Have a Bulletproof Vest: The National Security Risk Posed by the Lack of Cybersecurity in Implantable Medical Devices. Nova Law Review, 41(3), 419–448.

Yeng, P. K., D., S., & Yang, B. (2020). Legal Requirements towards Enhancing the Security of Medical Devices. International Journal of Advanced Computer Science and Applications, 11(11). https://doi.org/10.14569/IJACSA.2020.0111181