Volume 5 (2) 2023 https://doi.org/10.5204/lthj.3080

The Role of Cybersecurity in Medical Devices Regulation: Future Considerations and Solutions

Kaspar Rosager Ludvigsen
University of Edinburgh, United Kingdom

Abstract

The cybersecurity of medical devices is paramount in a world where everything is increasingly digitised. Attention to how this important defence against malicious actors is regulated must, therefore, also increase. This paper uncovers how the cybersecurity of medical devices is currently regulated and how it can be improved going forward. First, the paper compares the regulation of medical device cybersecurity in the European Union, the United States and the United Kingdom (UK)—differentiating between Great Britain and Northern Ireland as per the current state of the law in the UK. Second, the paper develops a model of how cybersecurity shapes three key areas in the ecosystem of medical devices. These areas are the medical device itself; the structure between the surrounding institutional systems (such as manufacturers and healthcare providers); and the security of the data, the surrounding institutional system and the medical device. Third, based on a comparative analysis and a view of the system from above, the paper puts forward four recommendations on what future regulation should contain to properly regulate the cybersecurity of medical devices: technology specificity, circumvention protection, genuine privacy and security by design. The paper recommends that these four principles be followed. Technology specificity because it guarantees legislation that understands the necessary technical aspects to promote security and safety. Circumvention protection because preventing manufacturers and others from circumventing these requirements decreases risks to the health and wellbeing of patients. Finally, genuine privacy and security by design should be followed to align cybersecurity and privacy with current and future technical capacities.

Keywords: Medical devices; EU Law; cybersecurity; policy; technology regulation.

1. Introduction[1]

Medical devices are becoming increasingly more sophisticated in a variety of ways. This includes having increasingly complex digital functionalities assisted by software systems.[2] This software can either be integrated into the device itself or as part of a wider digital systems ecosystem.[3] This move towards digitisation perhaps began earlier than expected, with digital pacemakers paving the way for digital implantable medical devices[4] and the increased adoption of surgical robots[5] and measuring tools.[6] Part and parcel with these developments is the fact that digital systems need to be safe and secure and, thus, must consider cybersecurity and privacy.[7]

[1] This paper was made possible by funding from the PETRAS RoasT-IoT project, and the UKRI TAS Governance node. I would like to thank the Everyday Cyborgs 2.0 project for the opportunity to present and write this paper, and additionally thank Muireann Quigley, Joseph T. F. Roberts, Laura Downey, and Zaina Mahmoud for their extensive feedback.

[2] For an alternative US-centric analysis of some of the issues this paper discusses, see Tschider, "Medical Device Artificial Intelligence."

[3] They may also become more autonomous, which requires additional considerations; see Danks, "Regulating Autonomous Systems"; Burton, "Mind the Gaps."

[4] Bains, "John Hopps and the Pacemaker."

[5] Leal Ghezzi, "30 Years of Robotic Surgery."

[6] Any type of measurement tool, be it IoT-based or not, are often considered medical devices because they aid in the diagnosis of diseases. These include digital elements; hence they are also part of this ongoing trend.

[7] Especially considering the vulnerable positions that modern medical devices put patients into; see Tschider, "Prescribing Exploitation."

Much like physical security—for example, protecting banks from robbers, civilians from each other or the integrity of physical messages[8], cybersecurity is necessary to prevent interference from cyberattacks (adversarial attacks). Cybersecurity protects what surrounds and exists inside the medical device against other human or automated attacks (adversaries). Whether an adversary succeeds in attacking a medical device or not, the privacy of what it contains or does to the patient should be protected. Privacy is a very broad concept, but for this paper, the focus is on the protection of confidentiality and the legal system that surrounds it, not how the term is defined in, for instance, Human Rights Law. Privacy for medical devices requires considering privacy-enhancing techniques (PETs)[9] and data protection law. Techniques, such as encryption, within privacy often overlap directly with cybersecurity, meaning that considerations for better security will also apply to privacy. This can be seen when it comes to confidentiality in cybersecurity,[10] which can be considered part of privacy, as there is a strong overlap between the two terms. Safety is also implicated in cybersecurity. Safety as a concept pertains to the prevention of accidents and losses[11] and represents the physical consequences that both breaches in cybersecurity and privacy can cause. Breaches in cybersecurity can lead to accidents or losses, while breaches in privacy can be used to cause either safety or security consequences; this means all three areas in practice strongly overlap. Broadly, we can say that safety applies universally, security requires adversaries and privacy requires personal data or a personal sphere.

Due to the possibility that medical devices can be vectors for cyberattacks, a more extensive and open debate regarding the concomitant risks their usage brings is necessary, as well as thoroughgoing discussions about what kind of function they should have in our society. Cyberattacks risk physical or financial damage but are preventable with adequate defences applied to both the medical devices themselves and their surrounding systems. Medical device cybersecurity may be approached in varied ways. For computer scientists, medical device cybersecurity poses specific problems not entirely different from the general issues of the Internet of Things (IoT)[12] or cyber-physical systems.[13] Adversaries use the same techniques such that the practical difference is minimal. In contrast, from a legal perspective, the specific cybersecurity of medical devices is regulated and understood separately from general cybersecurity. The explanation for the difference between the cybersecurity of medical devices and general cybersecurity comes from the severity of the consequences of their failure. This same concern can be seen in safety engineering, where perceptions and legal rules surrounding industries and products that can cause (physical) safety problems for the user or those the product is used on tend to be regulated more strictly.[14]

As medical devices are considered part of the critical infrastructure for most states (belonging to healthcare systems) while simultaneously considered products, their role in society must be examined. Cybersecurity is neither free in monetary terms nor free from conflict, and regulators' interests can clash strongly with manufacturers' interests. Cybersecurity developers have historically veered towards minimal compliance, while states prefer better cybersecurity than manufacturers would like to pay for.[15] In this way, device users and patients are between a rock and a hard place, as their interest is the protection of patient safety, security and privacy.[16]

To address these issues, this paper starts in section two by describing the current law. It details how medical device cybersecurity is regulated in the European Union (EU) and the United States of America (US), with comments on the law in Great Britain (GB). As will be explained in more detail later, this is to be distinguished from the United Kingdom (UK) as a whole since, following Brexit, the law concerning medical devices is different in GB—England, Wales and Scotland—than in Northern Ireland (NI). Here, I show that while some of the relevant laws in relation to medical devices do not seem to deal explicitly with cybersecurity, they do, in fact, contain provisions that ought to be interpreted as such. In section three, I expand the understanding of the cybersecurity of medical devices beyond a focus on the medical device itself. There, we see that it is imperative that the cybersecurity of medical devices is considered in tandem with that of their surrounding infrastructure and

[8] Dooley, "Cryptology Before 1500."

[9] Information Commissioner's Office, "Privacy-Enhancing Technologies (PETs)."

[10] Part of the so-called "CIA triad" in cybersecurity, confidentiality, integrity, and availability.

[11] Leveson, Safeware: System Safety and Computers, 181.

[12] IoT is a term that covers everything from smartwatches to network-connected surveillance cameras to sensors used in power plants. IoT devices must be simple—so things like smartphones and desktop computers are excluded—involve sensors and be network-connected. For more, see Chiara, "IoT and the New EU."

[13] Cyber-physical systems are defined as being able to interact with the surrounding environment, like surgical robots, doing so through measuring and understanding the environment they are in through sensors, and requiring network connectivity. See Fosch-Villaronga, "Cloud Robotics Law and Regulation."

[14] Though there may be disagreements as to what degree and what relationship safety should have with security; see Michalec, "When the Future Meets the Past."

[15] Ludvigsen, "Dissecting Liabilities"; Ludvigsen, "When Is Software a Medical Device?" For a similar US critique, see Johnson, "Closing the Cybersecurity Gap."

[16] Arguably, user (medical practitioner) protection of these three areas is also warranted, which is especially important when working with machines like surgical robots.

systems, something which needs to be considered when designing future laws and regulations. Having made this case, I then move on, in section four, to provide four recommendations that could improve medical device compliance and cybersecurity.

2. Legislative Landscape: Comparing the European Union, the United States and Post-Brexit Britain

To illustrate how different legal systems regulate medical device cybersecurity, I compare the solutions found in two of the major players in this area: the EU[17] and the US.[18] In addition, I examine the approach found in GB, which is now in a new position outside the EU trading block.[19] I do this for two interrelated reasons. First, as mentioned in the introduction, since Brexit, the UK's medical devices legislation now consists of two jurisdictions: NI, which continues to be governed by newer EU law in this respect, and GB, which, to all intents and purposes, is principally governed by the older EU Medical Devices Directive. In both NI and GB, this is achieved via different interpretations of the UK's Medical Devices Regulations 2002 (as amended). Second, as part of its new position outside the EU, GB is attempting to strike a balance between the approach of the EU and that of the US when it comes to medical devices, and it remains to be seen how successful this will turn out to be.
Let us start by looking at current EU law as it pertains to medical devices and cybersecurity therein.

2.1 The European Union: Safety and Performance as Cybersecurity?

Medical devices in the EU are currently regulated by the Medical Devices Regulation (MDR),[20] which reached full implementation in 2021. This replaced the Medical Devices Directive (MDD)[21] and the Active Implantable Medical Devices Directive (AIMDD).[22] To be considered a medical device, software or a cyber-physical[23] system must fulfil one of the requirements in Article 2(1):

> (1) '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[24]

These purposes are (1) diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease; (2) diagnosis, monitoring, treatment, alleviation of or compensation for an injury or disability; (3) investigation, replacement or modification of the anatomy or of a physiological or pathological process or state; (4) providing information by means of in vitro examination of specimens derived from the human body, organ, blood and tissue donations.[25] Within this definition, there is considerable uncertainty as to whether authorities will force products to be considered medical devices if they *de facto* function as such, but they may have the powers to do so.[26] However, a discussion of this here is beyond the scope of this article.

如果產品實際上具有醫療功能，當局是否會強制將其視為醫療裝置，這存在相當大的不確定性，但他們可能有權這樣做。

Interestingly, the MDR contains no provisions specifically labelled 'cybersecurity'. Without a mandated minimum cybersecurity requirement, manufacturers can lower the level of protection to decrease production costs. However, as will be shown, the General Safety and Performance Requirements (GSPR) for medical device functioning contained in Annex 1 can

[17] For alternative overviews, see Biasin, "Cybersecurity of Medical Devices"; Biasin, "AI Act Proposal."
[18] For older, non-cybersecurity focused comparisons, see Kramer, "Regulation of Medical Devices"; Altenstetter, "Medical Device Regulation Commonalities, Differences"; Chai, "Medical Device Regulation: Comparative Study."
[19] Green, "Medical Device Legislation Custom-Made Devices"; Han, "Opportunities and Risks."
[20] 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 L117/1.
[21] Council Directive 93/42/EEC of 14 June 1993 Concerning Medical Devices [1993] OJ L169/1.
[22] Although I do not explicitly deal with it here, an update to the in vitro rules also exists; see Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on In Vitro Diagnostic Medical Devices and Repealing Directive 98/79/EC and Commission Decision 2010/227/EU [2017] OJ L117/176.
[23] "Cyber-physical" refers to digital systems that interface with the physical world, usually in the form of actuators, such as with robots, or sensors, in the form of most IoT devices. The term is wide and mostly used in the engineering sphere but is more adequate when describing medical devices like surgical robots and pacemakers than just calling them hardware or digital systems.
[24] For more, see Ludvigsen, "Dissecting Liabilities." For an alternative approach that may capture medical devices too, see Roberts, "Prescribing Unapproved Medical Devices?"
[25] The MDR also includes devices that control or support conception, and cleaning/disinfection/sterilisation products used specifically for medical devices as accessories; see 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 L117/1, art 2(1).
[26] Such as Article 10(14) or 93. On this and the problem of intended use in medical devices, see Ludvigsen, "When Is Software a Medical Device?"

(for all intents and purposes) be read as such provisions.[27] Arguably, implementing cybersecurity in medical devices is necessary if manufacturers are not to violate their general obligations. The essential requirements in the MDR encompass various risk management systems, quality assurance and financial management,[28] and those set out in Annex 1, also called the GSPR. They also include the general idea that medical devices should not fail because of any type of adversary attacking them[29] and that the necessary cybersecurity for functioning must be in place.[30] The Medical Device Coordination Group (MDCG) has also published guidance on the MDR,[31] which contains elements that strongly promote good security, supporting the GSPR in Annex 1.[32]

The GSPR requirements are of special importance due to their wording of how a medical device's lifecycle should function. The consequence of this is that they, in effect, act as a way (albeit somewhat indirectly) to require adequate levels of cybersecurity. Let me explain in more detail. Take, for instance, Parts 17.2 and 17.4 in Annex 1. 17.2 requires that a device's software or software that is itself a medical device should be 'state of the art', with considerations as to its functioning, and 17.4 requires minimal security to prevent adversaries from interfering with medical devices working as intended. Given this, authorities in each Member State can use this safety and patient-focused text to mandate tight cybersecurity. They can do this by requiring a device's cybersecurity to be 'state of the art',[33] as well as ensuring that they function 'as intended', where 'as intended' is interpreted using cybersecurity standards.[34] This can be interpreted as requiring that medical devices resist enough cyberattacks to function under most circumstances, as the failure to do so could cause physical consequences, such as if surgical robots ceased to function while operating on patients or pacemakers halted their functioning. From a cybersecurity perspective, Parts 17.2 and 17.4 imply that a device must have good enough defences to deter anything but the most sophisticated adversaries; minimum levels of encryption, access control and physical cybersecurity must, therefore, follow.[35] An alternative interpretation requiring a lesser degree of protection would be contradictory; if manufacturers cannot guarantee the functioning of medical devices under or after expected adversarial attacks, they do not fulfil the GSPRs and, therefore, do not fulfil their obligations in Article 10 of the MDR.

The MDR safety and performance requirements do not stand on their own and, as such, need to be read in conjunction with different pieces of EU cybersecurity legislation, both current and forthcoming. While it is not necessary to get into the fine details of this legislation for the purposes of this paper, it is important to place the MDR cybersecurity implications into the broader legislative context. Current relevant legislation includes the Network and Information Systems (NIS 2) Directive[36] and the Cybersecurity Act.[37] The NIS 2 Directive, despite its name, is concerned with the cybersecurity of the general critical IT infrastructure of both private and public bodies across the EU and entails detailed legislation, guidance and enforcement to guarantee the safety and security of Member States and their citizens against adversaries. The NIS 2 Directive applies to all public and private bodies listed in Annex 1 and 2, which includes medical devices (Annex 1, point 5) as part of each Member State's healthcare sector, which in turn is considered critical infrastructure, such that legislation and practical implementation of security must be guaranteed, through strategies (Article 7), enforcement structures (Articles 8, 10, 20), and supervision

[27] Ludvigsen, "Dissecting Liabilities," 7–8.
[28] See 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 L117/1, art 10(2), 10(9), 10(1), (12)—(14), and 10(16).
[29] Strong adversaries may cause dismissal of liability in court for manufacturers; see Ludvigsen, "Dissecting Liabilities," 11–14.
[30] See 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 L117/1, art 10(2), 10(9), 10(1), (12)—(14), and 10(16). Some attacks can be considered unavoidable or close to it, and these include sophisticated attacks such as what was seen in the Stuxnet; see Falliere, W32.Stuxnet Dossier.
[31] Medical Device Coordination Group, MDCG 2019-16 Guidance on Cybersecurity.
[32] For additional commentary, see Ludvigsen, "Dissecting Liabilities"; Kamenjašević, "Commentary on Contact Proximity Tracing"; Granlund, "On Medical Device Cybersecurity Compliance."
[33] For a broader explanation of the role of this term, see Schmitz, "Conceptualising the Legal Notion."
[34] Ludvigsen, "Dissecting Liabilities," 8.
[35] For situations where implantable medical devices, or otherwise, may warrant less security, see Lindstad, "When Is the Processing of Data."
[36] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity Across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive) [2022] OJ L333/80.
[37] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [2019] OJ L151/15. This Act has no relevance for this paper, but empowers certain institutions within the EU, who can publish guidance and standards that may be relevant for the MDR and NIS 2 going forward.

(Articles 31, 32). However, as with the NIS 1 Directive,[38] there is a problem with implementation;[39] it is difficult to predict how Member States will build the systems necessary to comply with the NIS 2 Directive. The NIS 1 Directive was integrated into Member States in various ways,[40] which caused legal fragmentation. Since harmonisation across Member States is an organising principle within the EU, there is, thus, a significant concern about divergent approaches, something that remains with the NIS 2 Directive.

Two further pieces of proposed legislation also need to be considered. These are the Cyber Resilience Act (CRA)[41] and the Cyber Solidarity Act (CSA).[42] The CRA will improve and regulate the cybersecurity of any network-enabled devices, which in practice both applies to IoT devices and software. The MDR is *lex specialis,* but the CRA will also influence the cybersecurity requirements for medical devices, as many will have the same software or operating systems as those covered by the CRA. Additionally, the CRA is supposed to entail more resilience (greater recovery from failure), something that the MDR only vaguely mentions in its Annexes. The proposed CSA would create the European Cyber Shield (Article 3) consisting of interconnected security operation centres (set up by Articles 4 and 5) intended to develop the EU's capacity to detect cyber threats (Articles 4 and 5) and the Cyber Emergency Mechanism (Article 9) for which funding will be available to support actions intended to improve preparedness for, response to and mutual assistance for potential cybersecurity incidents (Article 10). These measures will knit the EU's cybersecurity tightly together and create emergency response mechanisms that can react when adversarial attacks threaten infrastructure or individuals across the union. This will improve the security of medical devices as well.

A potential issue across the EU's medical device cybersecurity framework generally is its use of, and reference to, security standards; for example, ISO 14155:2011.[43] The problem is not the use of security standards *per se*; it is the fact that most of them are developed by private actors, such as the International Organization for Standardization (ISO), who allow usage of the standard for a fee. Arguably, this creates an unnecessary barrier to the adequate protection of the health and safety of device users, as small or medium-sized enterprises will not necessarily have the resources to access the standards. The other issue, which there is no space to go into here, is the fact that these standards do not necessarily reflect best practice. They could represent compromised positions[44] or the positions of influential interested parties.[45] Both of these issues could be alleviated if the EU, specifically the European Union Agency for Cybersecurity, released Open Access standards that mimic or improve the existing ones.[46]

While the elements of the EU system just set out constitute the main framework relating to the cybersecurity of medical devices, the proposed Artificial Intelligence (AI) Act will also have a bearing on this area.[47] The AI Act regulates AI as a 'product'; it sets criteria for various risk classes, obligations of manufacturers and users, and the necessary testing bodies and authorities, similar to product legislation like the MDR. However, once implemented, this Act will create a host of issues regarding which rules apply, especially considering that the MDR has *lex specialis* status over medical devices.[48] Annex 2 reveals that AI used in or as medical devices will be considered high risk, with special categories for the management of risk in an AI setting.

[38] Directive (EU) 2016/745 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union [2016] OJ L194/1.

[39] Wallis, "Implementing the NIS Directive." The implementation in most member states has not gone as smoothly as the suggestions of this paper.

[40] For an example of three different implementations, see Ludvigsen, "Preventing or Mitigating Adversarial Supply." For a general overview, see Wallis, "Implementing the NIS Directive."

[41] Proposal for a Regulation of the European Parliament and of the Council on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulation (EU) 2019/1020 COM (2022) 454 final, 2022/0272 (COD). The Cyber Resilience Act explicitly excludes anything regulated by the MDR, but its concepts and systems may influence how medical devices could be regulated going forward. For analysis on the interplay of the CRA and NIS 2, see Eckhardt, "EU's Cybersecurity Framework."

[42] Proposal for a Regulation of the European Parliament and of the Council Laying Down Measures to Strengthen Solidarity and Capacities in the Union to Detect, Prepare for and Respond to Cybersecurity Threats and Incidents COM (2023) 209 final, 2023/0109 (COD).

[43] 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 L117/1, recital (64).

[44] Martinetti, "Redefining Safety."

[45] Teece, "Profiting from Innovation."

[46] This may be changing; see Advocate General's Opinion in Case C-588/21, where Advocate General Medina implies that if standards are used to design or even are part of the regulation, they should be freely available to those who use or need them. See also Andersdotter, "Policy Strategies for Value-Based Technology Standards."

[47] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM (2021) 206 final.

[48] For additional analysis on this, see Palmieri, "Blanket That Leaves the Feet Cold."

Despite this, AI in medical devices will mainly be regulated by the MDR.[49] The overlaps between the two pieces of legislation and arising conflicts could cause the risk of circumvention to be increased, such as the potential discussed earlier for developers to frame the intended purpose of their AI product to fall outside the MDR medical device definition and only adhere to the AI Act in a low-risk manner. The same AI could be considered high risk regardless of whether it is a medical device or not, whereas AI which are not medical devices will not be covered by the MDR. Conversely, the AI Act does contain cybersecurity Articles[50] that are specific and directly applicable to AI as medical devices. Considering its upcoming importance in all types of systems, it may serve as inspiration as to how other types of product legislation[51] should regulate cybersecurity in the future, in the form of dedicated staffing with specific professional skills regarding cybersecurity (Article 59(4)), and the explicit cybersecurity mentioned in Article 15. Finally, the cybersecurity of medical devices is also covered by the General Data Protection Regulation (GDPR),[52] which is structured around protecting the fundamental right to privacy, using data protection authorities, data protection officers and concepts like data controllers and data processors. The problem is that the GDPR is limited to considerations relating to personal data, meaning that the cybersecurity requirement cannot deal with all types of cybersecurity, which is possible with the legislation above. I now move to a very different system, the one seen across the Atlantic.

2.2 The United States: An Opaque and Arbitrary Regulatory Framework?

In the US, medical devices are governed federally[53] by section 201(h) of the Federal Food, Drug and Cosmetics Act.[54] The regulatory body is the Food and Drug Administration (FDA), which decides if devices fulfil the criteria to be considered medical devices and assesses the extent of their compliance with existing regulations.[55] No other cybersecurity rules apply directly and purely for medical devices, apart from an Executive Order (EO), which I will outline in due course.[56]

The US relies on *ex-ante* evaluations and approval over *ex-post* interventions, which has consequences for medical devices in the long term,[57] such as failure to account for vulnerabilities and issues with medical devices further developed and whose issues only show far after their approval. This can be seen if one looks at the example of IoT devices. These are simple devices with sensors and network connectivity, such as smart devices like cameras or sensors, or wearables, like pacemakers and automated insulin pumps, intended to be part of a greater system.[58] Manufacturers sometimes forgo updates to the software in IoT devices to cut costs, which, as time passes, makes them increasingly vulnerable to cyberattacks.[59] For this reason, the initial approval of a device does not ensure compliance throughout the medical devices' lifecycle. Thus, if there is no *ex-post* inspection, this can result in poor cybersecurity if not regularly serviced.[60]

As in the EU, there are no explicit mentions of cybersecurity in primary legal sources. However, the FDA's introduction of the Policy for Device Software Functions and Mobile Medical Applications,[61] as well as sections 3060 and 3060(a) of the 21st Century Cures Act,[62] require adequate cybersecurity to secure the correct functioning of medical devices, giving rise to more specific cybersecurity considerations. Much like the EU, for software to be considered a medical device by the FDA, the manufacturer must intend the software to be used to diagnose, cure, mitigate, treat or prevent disease or other conditions,[63] and

[49] This is the same for AI acting as an accessory to a medical device, as they must follow the same rules as the medical devices themselves; see 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 L117/1, art 1(1) and 2(2).

[50] Article 15 specifically, but other Articles like 14, and 63–68 will be important as well. For more detailed analysis of Article 15 of the AI Act see Biasin, "New Cybersecurity Requirements." For an analysis of AI-enabled medical devices in general, see Li, "Regulating Artificial Intelligence."

[51] The AI Act is also product legislation; for more on how this works out long term, see Almada, "EU AI Act: Between Product."

[52] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

[53] Note that while the regulation of cybersecurity of medical devices in general must comply with the minimum requirements from the FDA, additional rules on a State level may further complicate the process for manufacturers.

[54] https://www.fda.gov/medical-devices/classify-your-medical-device/how-determine-if-your-product-medical-device, last accessed 25 October 2023.

[55] Section 201(h) can also be found in 21 U.S.C. ch. 9 § 321(h)(1).

[56] There exists a range of general cybersecurity rules that apply generally, but these are not further analysed here.

[57] For an overview of the processes, see Tschider, "Deus Ex Machina," 19.

[58] See Michalec, "When the Future Meets the Past."

[59] Xenofontos, "Consumer, Commercial, and Industrial IoT (In)Security."

[60] Johnson, "Closing the Cybersecurity Gap."

[61] Food and Drug Administration, Policy for Device Software Functions.

[62] Food and Drug Administration, Changes to Existing Medical Software.

[63] 21 U.S.C. ch. 9 § 321(h)(1)(b).

its intended function must affect a bodily structure or function.[64] However, the FDA can also decide whether or not the software is a medical device regardless of the fulfilment of criteria.[65] This lets the FDA include *de facto* medical devices, even if they do not fulfil section 201(h), which prevents circumvention.

Medical devices may be classified at the FDA's discretion, where the products they support, as well as the centrality of the role of the software, influence where they belong.[66] This process is arguably opaque compared to the MDR, which, through its requirements, places more trust in the manufacturer to (mostly) initiate the certification and inspection process. This illustrates that the FDA's broad power in decision-making is one of the key differences between the US and the EU in regulating medical devices. The FDA can also forcefully withdraw devices from the market if they are not registered or are found to be noncompliant. This makes the FDA somewhat of an oracle since it is the sole centralised decider of the status of what is a medical device or not. This stands in contrast to the longer and more manufacturer-centric process in the EU.[67] Whether this centralised system functions appropriately is debated.[68] For example, Roth critiques the number of grey areas emerging from the current regulatory model, in part due to the FDA's arbitrary nature. He argues that if particular software or hardware is not deemed a medical device, then it will not be further regulated, potentially harming device users.[69] There is a paradox here, however. The centralised US system and the discretion afforded to the FDA may enable the FDA to recognise more *de facto* devices as medical devices and, thus, reduce the capacity for manufacturers to circumvent regulation. Nevertheless, that same discretion may also enable the increase in unregulated *de facto* medical devices such as chatbots or monitoring apps.[70] Additionally, there are limits to using non-binding instruments for tasks where hard law would be preferred.[71] It can lead to a more costly approvals process for manufacturers than under the MDR, where these decisions are governed by hard law, creating certainty for manufacturers.

Outside direct medical devices regulation, another regulatory mechanism to consider is EO 14017 on America's Supply Chains, which, in practice, created the basis for using a Software Bill of Materials (SBMs).[72] These documents must detail the technical cybersecurity measures used by the product and related services. This allows professionals and consumers to discern and understand what kind of encryption, security software or other types of cybersecurity protections are contained in the products. While not mandated for medical devices yet, outside procurement, where SBMs are mandatory, they could serve as an excellent tool to create higher levels of safety and security.[73]

Lastly, like the EU, the FDA employs guidance detailing cybersecurity, varying from informal to relatively detailed. Most relevant here is *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions Draft Guidance for Industry and Food and Drug Administration Staff*,[74] which provides manufacturers with expectations for inspection and approval. However, at the time of writing, detailed federal guidance for parties other than FDA staff is lacking. The same limitations that apply to data protection in the EU equally apply to the US law. There is limited federal protection and legislation that could require increased cybersecurity. Where this exists, it is instead done through specialised legislation like the Electronic Communications Privacy Act of 1986,[75] the Cybersecurity Act of 2015[76] and recently, the Cyber Incident Reporting for Critical Infrastructure Act of 2022[77] and the Strengthening American Cybersecurity Act of 2022.[78] Having detailed the centralised regulatory framework in the US, we can turn to examine the UK, or more specifically, GB.

[64] §321(h)(1)(c).
[65] §321(h)(1)(c).
[66] For a concrete overview, see their very accessible databases, Food and Drug Administration, "Product Classification."
[67] For past perspectives on this, see Chai, "Medical Device Regulation: Comparative Study."
[68] Roth, "How Much FDA Medical Device."
[69] Gallese, "Legal Issues," 413–414.
[70] Gallese, "Legal Issues."
[71] Gallese, "Legal Issues," 416.
[72] See papers such as Carmody, "Building Resilient Medical Technology Supply."
[73] As of the time of writing, the draft Cyber Resilience Act in the EU demands a Software Bill of Materials in Article 10(15). This may become relevant for the MDR going forward, as this requirement could be mimicked in guidance.
[74] Food and Drug Administration, Cybersecurity in Medical Devices.
[75] 18 U.S.C. ch. 119, 121, 206.
[76] 6 U.S.C. ch. 6.
[77] 6 U.S.C. ch. 1.
[78] Part of the Consolidated Appropriations Act 2022, Pub. L. No. 117-103, 136 Stat. 49 (2022).

2.3 Great Britain: Between a Regulatory Rock and a Hard Place?

Following Brexit, the regulation of medical devices now diverges between GB (England, Wales and Scotland) and NI.[79] As noted earlier, the principal provisions concerning medical devices in both NI and GB are contained in the UK's Medical Devices Regulations 2002 (as amended). However, there are two different interpretations contained within these: one pertaining to GB and one to NI. Through these, GB remains similar to its pre-Brexit status, the provisions in this respect reflecting the older MDD and AIMDD. However, due to its position outside the EU, GB now has an opportunity to create new divergent legislation.[80] Meanwhile, NI continues to follow EU law in this area and, therefore, is subject to the provisions of the EU MDR.[81] Since the EU MDR, and hence NI, was covered in section 2.1 above, I leave this aside for now and focus on GB.

The MDD, similarly to the MDR, lacks specific cybersecurity provisions and, as such, so too do the 2002 Regulations as they apply in GB. However, amendments to the 2002 Regulations could be interpreted such that manufacturers are required to show how their devices meet the essential requirements in the regulation in a way that creates additional indirect cybersecurity requirements, as seen in the MDR,[82] but only if the device does not already fulfil the requirements through compliance with international standards set out in Regulation 3A.[83] This may include indirect cybersecurity measures since the manufacturer is required to show how they meet the requirements of the 2002 Regulations if they have not used the aforementioned standards in 3A, in which the national authority could require cybersecurity measures. In addition to these modifications, past guidance[84] may apply in GB together with specific guidance from the UK Government.[85] The older guidance document MEDDEV 2.1/6 is very sparse in its cybersecurity details, leaving most of the related regulations up to the government, where they are found in specialised guidance, which then is only acted upon if any of the enforcement structures in the 2002 Regulations are applicable. The risk is whether there will be compliance adherence before any damage is done, like in the surgical mesh incidents in the UK.[86]

Post Brexit, the government launched a public consultation on the future path that the Medical Device Regulations should take,[87] which provided detailed suggestions for changes. Of special note is the commitment from the government to include cybersecurity as an essential requirement,[88] but such a commitment is noticeably lacking elsewhere in the government's response to the consultation. The emerging problem for GB will be the barriers to export and import; devices purchased in and placed on the EU market will need to conform with the rules discussed above (section 2.1), and devices purchased in and placed on the US market will need to conform with US requirements (2.2) and often EU law,[89] leaving little room for GB law to practically diverge. This is increasingly apparent when looking at cybersecurity, which remains unchanged notwithstanding Brexit; breaches, exploits and other attacks will keep requiring new defences that transcend borders and affect all countries equally. Keeping standards broadly similar across most countries would prevent the worst breaches from spilling into other states, which is especially prudent regarding medical devices, as they can cause physical damage and human injury from cyberattacks.[90] It would also allow medical devices produced in the UK to be easily exported. This sentiment is not reflected in the government's response to the public consultation or the recent changes to the 2002 Regulations; nevertheless, the UK Government has the option to consider aligning its rules closer to either EU or US law or both. In the same vein, data protection in the UK suffers from the same disadvantages as the two above, and its cybersecurity protection does not extend beyond personal data, making specialised legislation necessary.

[79] For more detailed account of the regulatory framework in the UK, see Quigley, "Future of Medical Devices Regulation."

[80] Whether this will end well is debated, see Han, "Opportunities and Risks."

[81] See Agreement on the Withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community [2019] OJ C 384 I/01.

[82] Agreement on the Withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community [2019] OJ C 384 I/01, sch 2A, pt 2, para 14(e), 4.2. This comes from the Medical Devices (Amendment etc.) (EU Exit) Regulations 2020 sch 2, para 56.

[83] See the Medical Devices Regulations 2002, Part 2, sch 2A, pt 2, para 14€, which substitutes in new Parts 4.1, 4.2, and so forth into Annex 3 of Directive 93/42/EC. See also the Medical Devices (Amendment etc.) (EU Exit) Regulations 2020 reg 3(6).

[84] European Commission, Guidelines on the Qualification and Classification. This guidance was initially important in determining and understanding cybersecurity requirements for all medical devices.

[85] This could be the following: GOV.UK, "Regulating Medical Devices in the UK."

[86] The Independent Medicines & Medical Devices Safety Review, "First Do No Harm."

[87] Medicines & Healthcare products Regulatory Agency, Government Response.

[88] Medicines & Healthcare products Regulatory Agency, Government Response, 116.

[89] Due to the Brussels effect, see papers such as Bygrave, "'Strasbourg Effect' on Data Protection."

[90] See, for example, Al Momin, "Teleoperated Surgical Robot Security."

3. The Case for a Wider Systems Approach to Medical Devices Cybersecurity Regulation

None of the jurisdictions discussed have medical device–specific cybersecurity legislation, and all rely greatly on guidance. They also rely heavily on manufacturers to ensure the safety of their products. EU and GB law (in different ways, as shown above) use a combination of GSPR, guidance and trust in manufacturers, while US law centrally decides via the FDA and uses informal guidance to a much larger extent.

In the previous section, I noted several weaknesses with the different approaches. Key among these is uncertainty about enforcement, either through manufacturer-centric rules (EU) or central authority decisions (US); a fragmented regulatory state that leaves cybersecurity to voluntary or indirect effort (GB and NI law); and a lack of concrete cybersecurity provisions in the main body of law (all three jurisdictions). The latter is their shared central problem. While delegation to separately controlled specialised legislation is necessary, this does not prevent the product legislation needed for medical devices regulation from containing explicit cybersecurity provisions. Further, cybersecurity provisions in data protection law do exist in all three jurisdictions, but there will not always be (personal) data to protect or privacy issues, leading to a lack of regulatory capture.

This section explores how these weaknesses might be addressed by future regulations on the cybersecurity of medical devices. To do so, I revisit some key points relating to medical devices' cybersecurity. What will be seen more explicitly in this section is that, for medical devices' cybersecurity to be tackled in a more thoroughgoing way, regulation needs to take better account not only of the devices themselves but also the infrastructures and systems in which they sit.

Let us cast our minds back to the discussion of the cybersecurity of medical devices in the three jurisdictions in the previous section. They all make use of guidance, not the main body of law, to create cybersecurity obligations. They mostly use GSPR concepts, like 'functioning', which is different from good or 'state of the art' cybersecurity. Cybersecurity measures necessary for a device to function do not include systems that can guarantee the security or the safety of a patient in case of sophisticated or intrinsic cyberattacks, but it is likely that 'state of the art' does, as it implies a higher standard that is constantly improved. This means that to improve cybersecurity, future regulations could consider more specific provisions that are closer to how cybersecurity is done in practice. Further, medical devices require data to function. This can be generated by the devices themselves, from healthcare institutions or other sources. Arguably, cybersecurity properly conceived ought to also protect this aspect. Normally, privacy and data protection (two different topics) are regulated distinct from cybersecurity concerns. For instance, the GDPR governs all aspects of data in the EU and has certain requirements regarding the security of the processing and storage of personal data.[91] Finally, cybersecurity also includes the entire system surrounding what you intend to protect, which means that the cybersecurity of hospitals, wards, manufacturers (data or analysis from them may be central) and even individual professional users should be considered. None of the three jurisdictions do this specifically in medical device legislation.[92]

Given all of this, I posit three domains of concern regarding the cybersecurity of medical devices. My suggestion is that each of these, and the interrelations between them, needs to be attended to in any future regulations if cybersecurity is to be taken seriously and properly enacted. As will be seen from the description given and the accompanying graphics, these domains can be conceptualised as nested layers, where 'domain' is an expansion on the one below it but where achieving adequate cybersecurity of the system as a whole is not possible without taking these wider elements into consideration. The three domains are as follows:

- Domain **1** encompasses the actual safety and cybersecurity techniques within medical devices.
- Domain **2** relates to protection against adversarial attacks from third parties, including authorities, manufacturers and cybersecurity providers themselves. Cybersecurity protection to ensure the risk of manipulation or alteration of medical devices is minimised. No regulation provides this level of protection, and due to the nature of these devices, it is imperative that protection aims to prevent or at least attempts to mitigate various types of adversarial attacks from all, including manufacturers. If protection against manufacturers seems surprising, it is important to keep in mind that these are still commercial products, and customisation or alternative use is rife, as seen with open-source solutions to everything from medical devices[93] to insulin production.[94]

[91] See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L1191, art 32. See also Schmitz-Berndt, "Don't Tell Them Now."

[92] However, they do consider cybersecurity of critical infrastructure, as shown with NIS 1 and NIS 2 above.

[93] Roberts, "Prescribing Unapproved Medical Devices?"

[94] Burnside, "Open-Source Automated Insulin Delivery"; Lum, "Real-World Prospective Study."

- Domain **3** goes further and includes privacy and security measures safeguarding the entire ecosystem in which medical devices exist, where data is necessary for functioning. This means that the cybersecurity of hospitals and manufacturers, who may provide server or analysis functions for software or IoT devices, are included in this type of system.

These domains expand the consideration of medical device cybersecurity from concentrating on the device alone to taking into account wider systems issues, such as communication beyond the device itself and interactions with the wider system. It also recognises the importance of data within the system and its relationship to overall cybersecurity considerations.[95] For an illustration of the relationship between these aspects, see Figure 1.

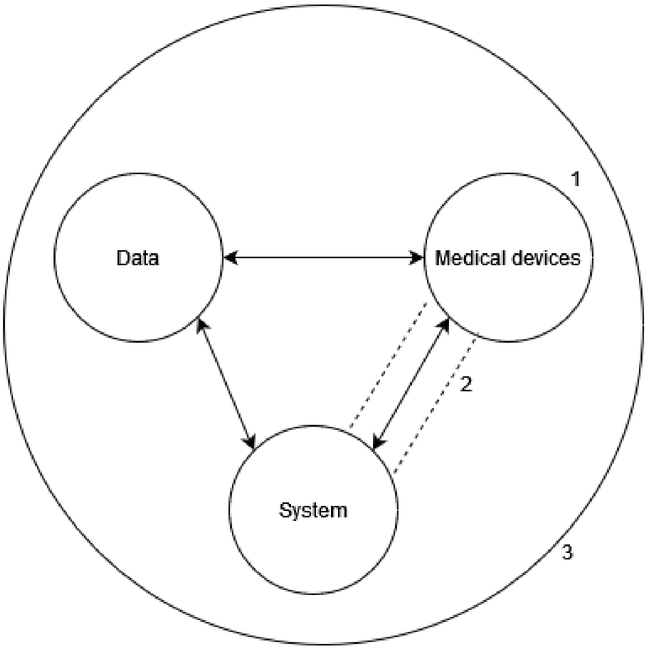

Figure 1. Three-Levelled Cybersecurity Structure for Medical Devices

To achieve the protection envisaged, especially in Domain 3, the necessary cybersecurity should be separately protected going forward, as the amount of analysis and outcomes with access to either part of this ecosystem only enlarges with time, thereby increasing the risk of harm to the patient. Adequate privacy protection should not harm the patient in a material or physical manner and should go beyond the GDPR and specialised data protection legislation, such as the proposed European Health Data Space Regulation offer.[96] How this could work in practice is discussed later.

Having made the case that an adequate regulatory approach would consider not only medical devices themselves but also the infrastructures and systems that surround them, in the next section, I make four specific recommendations for reform that could be beneficial should they be taken up by regulators. These are not limited to any jurisdiction and serve as inspirational points taken from both law and cybersecurity.

[95] Cybersecurity practitioners already view the security of medical devices in this manner, as they do not significantly diverge from other types of devices. The specific encryption, access control, or other protections needed for a surgical robot, are similar to what is seen in industrial robots, and pacemakers have similar protection to IoT devices such as wearables.
[96] Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space COM (2022) 197/2, 2022/0104 (COD).

4. Recommendations for Reform

These recommendations are specifically for usage in positive regulation, be it primary legislation or statutory instruments. For reasons I am about to elaborate on, they are not aimed at guidance, standards or soft law.

4.1 The Issue of Standards: Checkbox Exercises or Something Else?

Standards are commonly mentioned as a means to regulate technology.[97] Standards are documents that describe, either in detail or abstractly, how systems should be designed, run or discontinued. Most standards are maintained and provided by for-profit companies and are, as such, themselves products. Further, standards do not always reflect best practice and may be poor according to those who are supposed to use them.[98] This is also the case regarding cybersecurity, meaning that to use them as the sole—or even principal—basis of regulation would be unwise. As for medical devices specifically, the use of standards is more accepted, but this may be because of their focus on safety, reliability and general functioning rather than cybersecurity. Moreover, they do not describe most medical devices in technology-specific detail, rendering them more as guidelines instead. In this article, therefore, I do not recommend using standards instead of regulation. Even if the relevant standards were to be maintained and provided by the state or the EU, as they amount to essentially detailed guidance, they can never be a primary source of law and, thus, could be changed too easily. While flexibility can be an advantage, allowing standards or guidance to change if technology changes, it can have severe consequences if inadequately written.

In thinking about recommendations for reform, it is necessary to think about what different stakeholders want in this area: developers, designers and other elements of the (cyber)security economic landscape. Solutions to complex problems must be manageable, easy and suitable to implement and deploy in practice. First, such solutions exist for cybersecurity,[99] with easy-to-implement end-to-end security and privacy solutions.[100] Additionally, equally affordable next-generation encryption is close.[101] Second, every party imaginable, except for the state perhaps,[102] would want clear and easily applicable legislation. The state is an exception, as it often holds the power to certify or inspect devices and has a monopoly on surveillance, both of which could violate patient confidentiality and integrity. Legislation mandating poor cybersecurity to facilitate state surveillance indicates that states are not necessarily interested in good cybersecurity. Examples of this include the Online Safety Bill in the UK and the Child Sexual Abuse Regulation in the EU. With cybersecurity, any backdoor for the state is a backdoor for any adversary, decreasing patient safety.

Lastly, and regardless of the specifics of any legal system, the means to circumvent cybersecurity requirements exists, both practically speaking and from a regulatory perspective. However, there are possible paths to prevention or deterrence. Such prevention is desirable as circumvention or malicious noncompliance could lead to device user harm, for instance, if an adversarial attack were to be successful in manipulating a surgical robot.[103] If medical devices become even more connected and use even more digital elements in the future, the ways in which circumvention of cybersecurity provisions is prevented should increase proportionally.

To this end, I, therefore, make legislative recommendations in four areas. These are technological specificity, circumvention protection, genuine privacy and security by design. Let us examine each of these in turn.

[97] For some relevant perspectives, see Leverett, Standardisation and Certification of Safety; Andersdotter, "Policy Strategies for Value-Based Technology Standards"; O'Sullivan, "Legal, Regulatory, and Ethical Frameworks"; Clark-Ginsberg, "Regulating Risks within Complex Sociotechnical"; Teece, "Profiting from Innovation"; Danks, "Regulating Autonomous Systems."

[98] See, for example, Abelson, "Bugs in Our Pockets," 25.

[99] There are promising effects of end-to-end encryption in this area; see Quamara, "End-to-End Security Framework"; Strielkina, "Cybersecurity of Healthcare IoT-Based Systems."

[100] Homomorphic encryption and follow-up techniques may be the way to go, but the techniques are not silver bullets either; see Corrales Compagnucci, "Homomorphic Encryption."

[101] Though it is more complicated than it seems; see, for example, Atik, "Quantum Computing and Computational Law."

[102] As a general principle in cybersecurity, any backdoors created for state authorities will always be used by other adversaries, such as foreign actors or criminals, which historically can be showcased with things like keys escrow; see Abelson, "Bugs in Our Pockets."

[103] See, for example, Bonaci, "Experimental Analysis of Denial-Of-Service Attacks."

4.2 Technology Specificity

Legislation tends to fall on a spectrum from technology-neutral to technology-specific.[104] Neutrality, in this instance, refers to the broad applicability of the legislation regardless of the technology used.[105] A particularly well-accepted example of this is the GDPR. However, broad applicability comes at a cost; that is, a lack of explicit and specialised provisions directly regulating specific areas. Where this occurs, the vaguely worded provisions of a piece of technology-neutral legislation are frequently left to the courts to be interpreted. Alternatively, further detail is fleshed out in secondary legal sources, such as guidance, standards and so on, which can be blindly followed but not referred to by the primary legislation or simply through contractual specifications. The difficulty with this is that it creates fragmentation. By contrast, technology-specific regulation directly regulates specific areas. Telecommunication regulation is a good example thereof.[106] The proposed EU AI Act is another example specifically drafted to regulate specific types of software. However, a built-in weakness of this approach is in the particular definitions chosen. This is because their specificity makes circumvention or noncompliance by manufacturers easier,[107] though authors note that this may be just as true for technology-neutral legislation.[108] Medical devices legislation, by its very nature, is already technology specific. Nevertheless, as it currently stands, it lacks specificity when it comes to its cybersecurity requirements. Despite the potential weaknesses of technology-specific approaches just mentioned, this should be the norm going forward regarding medical device cybersecurity regulation. There are several reasons for this.

First, if there were stringent cybersecurity requirements, there would be no ‘legacy device’ problems (e.g., medical devices still in use with outdated operating systems such as Windows XP),[109] meaning more would pass regular screening or inspections necessary for good security. Second, stringent requirements would set expectations high; for manufacturers, expecting good cybersecurity on all three domains from Figure 1 explicitly in the legislation would guarantee larger considerations of patient safety and security. Third, technology-specific regulation understands its subject, something that technology-neutral regulation cannot (because it must fit all things possible).[110] Using technology-specific regulation could, therefore, mean that cybersecurity and privacy can be understood in a relevant manner and not in speculative ways, such as focusing too much on quantum cybersecurity, while most cyberattacks will be based on social engineering (phishing).[111]

4.3 Circumvention Protection

Bad Man’s Law is a well known and widely used concept in law, used to outline potential shortcomings in legislation.[112] It is used to refer to the fact that how the law is written and how people act with respect to the law may be different. As such, the putative ‘bad man’, instead of following the law, may find ways to circumvent it or to be otherwise noncompliant with its requirements. Bad Man’s Law as a concept showcases how noncompliance is a constant threat to any legal rule or system. As a legal principle, it has found varying degrees of penetration within EU Member States, being used in some while ignored in others, despite appearing in several cases.[113] When used in this way, it essentially refers to the practice of pretending to comply with the rules while, in practice, not doing so and enjoying advantages from this fraudulent scheme,[114] something that the European Court of Justice has declared is prohibited within EU law.[115]

[104] Koops, “Should ICT Regulation Be Technology-Neutral?”; Ohm, “Argument against Technology-Neutral Surveillance Laws”; Reed, “Taking Sides on Technology Neutrality”; Hojnik, “Technology Neutral EU Law.” Technology-specific regulation already exists in areas like telecommunication in all three jurisdictions.

[105] Medical device legislation, by its very nature, is in general already technology specific within the criteria mentioned in this paper. Nevertheless, it lacks specificity when it comes to its cybersecurity requirements, which should be the norm going forward.

[106] See, for example, Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 Establishing the European Electronic Communications Code [2018] OJ LL321/36.

[107] See Reed, “Taking Sides on Technology Neutrality,” 284.

[108] Koops, “Should ICT Regulation Be Technology-Neutral?”; Ohm, “Argument against Technology-Neutral Surveillance Laws”; Reed, “Taking Sides on Technology Neutrality”; Hojnik, “Technology Neutral EU Law.”

[109] Johnson, “FDA Regulation of Medical Devices”; Johnson, “Closing the Cybersecurity Gap.”

[110] Finally, the classic problem of “lagging behind” is not discussed. There are numerous articles that look specifically at this, including those, such as Reed, “Taking Sides on Technology Neutrality,” who argue that it is not in fact an issue due to, for example, the interpretative mechanisms given by courts, or secondary legal sources.

[111] Bullée, “Social Engineering.”

[112] Twining, “The Bad Man Revisited”; Jimenez, “Finding the Good.”

[113] For example, Case C-255/02, Halifax plc and Others v. HM Customs & Excise, 2006 EU:C:2006:121, para 68. See also Joined Cases C-59/13 and C-58/13, Angelo Alberto Torresi and Pierfrancesco Torresi v. Consiglio dell’Ordine degli Avvocati di Macerata, 2014 ECLI:EU:C:2014:2088.

[114] Joined Cases C-59/13 and C-58/13, Angelo Alberto Torresi and Pierfrancesco Torresi v. Consiglio dell’Ordine degli Avvocati di Macerata, 2014 ECLI:EU:C:2014:2088, paras 41–42.

[115] This must be tested, done in Joined Cases C-59/13 and C-58/13, *Angelo Alberto Torresi and Pierfrancesco Torresi v. Consiglio dell’Ordine degli Avvocati di Macerata*, 2014 ECLI:EU:C:2014:2088, paras 45–46.

Extrapolating this principle to medical device cybersecurity regulation would be advantageous. At the time of writing, an explicit principle like the one indicated here does not exist in GB and US law. This could prevent manufacturers from pretending to have good security while deploying poor cybersecurity to cut costs, risking the health and wellbeing of patients and medical staff. Explicit legislation to these ends would minimise the risks caused by poor security and, thus, ensure that medical devices are safe and usable. Safety requires strong enough cybersecurity to prevent potential adversaries from causing safety failures. To ensure this, additional measures to prevent circumvention, akin to what can be interpreted to exist in the EU MDR, are needed. In section 2.1, we saw that GSPR rules in Annex 1 could mandate stronger cybersecurity to maintain the functioning of medical devices—this implies safe functioning. Guaranteeing safety and security through functioning could then be a requirement in the medical device legislation, something that all three jurisdictions showcased in this paper lack.

4.4 Genuine Privacy

As standardly discussed in various literature, privacy is said to require trade-offs.[116] For instance, it is commonly thought that one cannot have both good privacy regarding the data and usage of medical devices without trading this off against issues with the software or hardware. This could be in the form of issues with access or excessive resources to achieve such privacy, but this is less of an issue now and likely will not be an issue in the future. New techniques, such as so-called quantum encryption, may be futureproof if combined with existing conventional defences. If this is so, devices that are continuously in use, even over the course of a decade or longer, may still retain some protection against adversaries. One implication of this is that medical devices regulation should mandate greater privacy, as the technology that can be used to do so will be easy to implement going forward. However, to properly ensure privacy as part of cybersecurity requirements, technology-specific legislation could mandate certain types of encryptions or PETs.[117] Finally, because such systems would allow for data usage without compromising privacy, states would still be able to analyse and survey the medical device ecosystem. This would be beneficial because it allows states to retain surveillance monopolies while giving the patient much greater technical privacy protection and could allow further analysis of the data through concepts such as sandboxes[118] or health data libraries.[119]

4.5 Security by Design

We have already seen that the EU's GDPR is a good example of a technology-neutral piece of legislation. It is also an excellent example of legislation that introduces 'privacy by design'.[120] Privacy by design is the idea that the technologies and internal design necessary to preserve the privacy of the data subject are baked into the development of the device from conception. The idea of using technology to design principles, values or regulatory requirements can also be found in the EU's CRA[121] in a security context. The CRA, which we met in section 2.1, mandates that security must also be built in and considered for the design of network-connected devices and systems, mirroring the privacy by design concept. The advantages of designing security in this way are that it likely increases general cybersecurity, limits risky decision-making by manufacturers concerning security and allows for easier auditing, as a lack of security by design is clear when it fails. However, such measures are not required for medical devices in any of the jurisdictions discussed in this paper. There is no technical barrier to requiring security by design for medical design manufacturers, and the literature supports increasingly implementing better security due to their decreased costs and ease of implementation. Further, requiring security by design would mirror the GSPR elements that all three jurisdictions in this paper already use.

Keeping cybersecurity an integral part of the design, function and maintenance of medical devices seems wise, considering their increasing level of digitisation, which is accompanied by an increased risk of adversarial attacks. Security by design ensures that good security cannot be substituted by secrecy.[122] Relying on secrecy is unsafe, as any adversary discovering the

[116] This was noted very early, before computers existed; see Kerckhoffs, "La Cryptographie Militaire."

[117] Done in practice in the EU but could be mandated by law too. For more, see Phillips, "Privacy Policy and PETs." GB and US law have not, as of the time of writing, embraced requiring PETs in legislation yet, but it sees use in guidance; see, for example, Information Commissioner's Office, "Privacy-Enhancing Technologies (PETs)."

[118] Seen in, for example, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM (2021) 206 final, 2021/0106 (COD), art 53. Sandboxes are here "playgrounds" where machine-learning or other types of software can be tested in protected datasets and refers in general to the idea of experimentation in CS circles.

[119] See Abelson, "Bugs in Our Pockets," which builds its entire concept on this.

[120] See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L1191, art 25.

[121] Proposal for a Regulation of the European Parliament and of the Council on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulation (EU) 2019/1020 COM (2022) 454 final, 2022/0272 (COD).

[122] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM (2021) 206 final, 2021/0106 (COD), art 53.

secret can then abuse it. Conversely, cybersecurity that is thoroughly tested but well known is the standard for complicated encryption systems,[123] so that the security used should be thoroughly tested and as impervious as possible, even if the adversary knows the techniques used. Notwithstanding the need for emergency overriding measures with implantable medical devices, like pacemakers, that create exploitable weaknesses,[124] those who design and deploy medical devices must strive towards the greatest level of cybersecurity. As with privacy, if security techniques become better and cheaper to implement, then their usage should proportionally increase.[125]

5. Conclusion

This paper set out to analyse and compare EU (including NI) and US law, with some commentary on GB, with the goal of providing a new model to understand medical device cybersecurity and suggest recommendations for future medical device cybersecurity regulation. As part of this, we saw that current EU law has changed since the new MDR, with legislation directly impacting medical devices. Yet despite this recent change to medical devices regulation, there are no explicit 'cybersecurity' provisions. Nevertheless, due to the influx of new cybersecurity legislation and existing guidance and medical device safety/functioning rules in the EU MDR, the regulatory landscape, including GSPR, is promising. In the US, the approval process and evaluation are still within the FDA's remit, with little testing or inspection after approval. Like the EU, the US lacks explicit cybersecurity provisions, but guidance reveals that the FDA is well-equipped to review medical devices and their cybersecurity properly before they are put on the market. However, it should be noted that they rarely follow up later.[126] Finally, the Medical Devices Regulation 2002, as applied to GB law, retains implementation of the older MDD and AIMDD, with little change since Brexit. Meanwhile, NI is subject to the provisions of the EU MDR. As cybersecurity is a global issue, there is little leeway for diverging innovative regulation in GB, and the UK Government should choose a regulatory path going forward that enables the easy export of medical devices. However, such a pathway seems unclear in the government's response to the recent public consultation on the future of medical devices regulation in the UK.

Having explored the weaknesses of the regulation in the three jurisdictions, I then presented a systems-based view of the cybersecurity of medical devices in a model depicting three domains of concern relating to medical device cybersecurity protection (presented in Figure 1). These include the actual safety and security techniques within medical devices, protection against adversarial attacks and the system as a whole. In taking a much wider approach to cybersecurity than a narrow focus on the device itself, this model serves to remind policymakers and manufacturers that cybersecurity properly conceived has to involve considerations of different interconnected domains. This is something that they would be well advised to note in any future regulations in this area.

Finally, based on the three spheres above, four recommendations for the future regulation of cybersecurity in medical devices were suggested: technology specificity, circumvention protection, genuine privacy and security by design. The first two are inspired by existing concepts and understandings of how policy should be built. Technology specificity is necessary because of the ever-increasing need for good cybersecurity in medical devices, while circumvention protection is necessary because noncompliance poses a bodily threat to patients if basic cybersecurity practices cannot be followed. The last two represent developments in technology warranting revaluations on what is acceptable to require through regulation. Genuine privacy comes from the idea that both now and going forward, good PETs allow for protection against actors who would threaten the privacy of the patient, which should be mandated by law. Security by design does the same in a cybersecurity context, as good security techniques are not as financially or computationally expensive as they used to be. The recommendations and the system-based view are good introductions to the complexity of this kind of regulation, but they also give a clear path towards a future with safer and more secure medical devices.

[123] Anderson, Security Engineering.

[124] This is debatable in the context of existing vulnerabilities, see Kramer, "Cybersecurity Concerns and Medical Devices"; Baranchuk, "Cybersecurity for Cardiac Implantable Electronic."

[125] Bhuyan, "Transforming Healthcare."

[126] Johnson, "Closing the Cybersecurity Gap."

Bibliography

Abelson, Hal, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Jon Callas, Whitfield Diffie, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Vanessa Teague and Carmela Troncoso. *Bugs in Our Pockets: The Risks of Client-Side Scanning*. October 14, 2021. http://arxiv.org/abs/2110.07450.

Almada, Marco and Nicolas Petit. *The EU AI Act: Between Product Safety and Fundamental Rights*. (Robert Schuman Centre for Advanced Studies Research Paper No 2023/59, 2022).

Al Momin, Md Abdullah and Md Nazmul Islam. "Teleoperated Surgical Robot Security: Challenges and Solutions." In *Advances in Web Technologies and Engineering*, edited by Xiali Hei, 143–160. IGI Global, 2022. https://doi.org/10.4018/978-1-7998-7323-5.ch009.

Altenstetter, Christa. "Medical Device Regulation in the European Union, Japan and the United States. Commonalities, Differences and Challenges." *Innovation: The European Journal of Social Science Research* 25, no 4 (2012): 362–388. https://doi.org/10.1080/13511610.2012.723328.

Andersdotter, Amelia and Lukasz Olejnik. "Policy Strategies for Value-Based Technology Standards." *Internet Policy Review* 10, no 3 (2021). https://doi.org/10.14763/2021.3.1573.

Anderson, Ross. *Security Engineering: A Guide to Building Dependable Distributed Systems*. Hoboken: John Wiley & Sons, 2020.

Atik, Jeffery and Valentin Jeutner. "Quantum Computing and Computational Law." *Law, Innovation and Technology* 13, no 2 (2021): 302–324. https://doi.org/10.1080/17579961.2021.1977216.

Bains, Perminder, M. Ignaszewski, S. Ladhar and Matthew Bennet. "John Hopps and the Pacemaker: A History and Detailed Overview of Devices, Indications, and Complications." *BC Medical Journal* 59, no 1 (2017).

Baranchuk, Adrian, Marwan M. Refaat, Kristen K. Patton, Mina K. Chung, Kousik Krishnan, Valentina Kutyifa, Gaurav Upadhyay, John D. Fisher and Dhanunjaya R. Lakkireddy. "Cybersecurity for Cardiac Implantable Electronic Devices." *Journal of the American College of Cardiology* 71, no 11 (2018): 1284–1288. https://doi.org/10.1016/j.jacc.2018.01.023.

Bhuyan, Soumitra Sudip, Umar Y. Kabir, Jessica M. Escareno, Kenya Ector, Sandeep Palakodeti, David Wyant, Sajeesh Kumar, Marian Levy, Satish Kedia, Dipankar Dasgupta and Aram Dobalian. "Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations." *Journal of Medical Systems* 44, no 5 (2020): 98. https://doi.org/10.1007/s10916-019-1507-y.

Biasin, Elisabetta and Erik Kamenjašević. "The AI Act Proposal, the Reform of the NIS Directive and the New Medical Devices' Cybersecurity Challenges in the European Union." *International Cybersecurity Law Review*, no 3 (2022): 163–180. https://doi.org/10.1365/s43439-022-00054-x.

Biasin, Elisabetta and Erik Kamenjašević. "Cybersecurity of Medical Devices: Regulatory Challenges in the EU." In *The Future of Medical Device Regulation: Innovation and Protection*. United Kingdom: Cambridge University Press, 2020. http://doi.org/10.2139/ssrn.3855491.

Biasin, Elisabetta, Erik Kamenjašević and Burcu Yaşar. "New Cybersecurity Requirements for Medical Devices in the EU: The European Health Data Space Regulation, Data Act, and Artificial Intelligence Act Proposals." *Law, Technology and Humans* 5, no 2 (2023). 43-58. https://doi.org/10.5204/lthj.3068.

Bonaci, Tamara, Junjie Yan, Jeffrey Herron, Howard Jay Chizeck and Tadayoshi Kohno. "Experimental Analysis of Denial-Of-Service Attacks on Teleoperated Robotic Systems." In *Proceedings of the ACM/IEEE 6th International Conference on Cyber-Physical Systems (ICCPS '15),* 11–20. New York: Association for Computing Machinery, 2015. https://doi.org/10.1145/2735960.2735980.

Bullée, Jan-Willem and Marianne Junger. "Social Engineering." In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, edited by Thomas J. Holt and Adam M. Bossler, 849–875. Cham: Springer International Publishing, 2020. https://doi.org/10.1007/978-3-319-78440-3_38.

Burnside, Mercedes J., Dana M. Lewis, Hamish R. Crocket, Renee A. Meier, Jonathan A. Williman, Olivia J. Sanders, Craig A. Jefferies, Ann M. Faherty, Ryan G. Paul, Claire S. Lever, Sarah K. J. Price, Carla M. Frewen, Shirley D. Jones, Tim C. Gunn, Christina Lampey, Benjamin J. Wheeler and Martin I. de Bock. "Open-Source Automated Insulin Delivery in Type 1 Diabetes." *New England Journal of Medicine* 387, no 10 (2022): 869–881. https://doi.org/10.1056/NEJMoa2203913.

Burton, Simon, Ibrahim Habli, Tom Lawton, John McDermid, Phillip Morgan and Zoe Porter. "Mind the Gaps: Assuring the Safety of Autonomous Systems from an Engineering, Ethical, and Legal Perspective." *Artificial Intelligence* 279 (2020): 103201. https://doi.org/10.1016/j.artint.2019.103201.

Bygrave, Lee A. "The 'Strasbourg Effect' on Data Protection in Light of the 'Brussels Effect': Logic, Mechanics and Prospects." *Computer Law & Security Review* 40 (2021): 105460. https://doi.org/10.1016/j.clsr.2020.105460.

Carmody, Seth, Andrea Coravos, Ginny Fahs, Audra Hatch, Janine Medina, Beau Woods and Joshua Corman. "Building Resilient Medical Technology Supply Chains with a Software Bill of Materials." *npj Digital Medicine* 4, no 1 (2021): 34. https://doi.org/10.1038/s41746-021-00403-w.

Chai, John Y. "Medical Device Regulation in the United States and the European Union: A Comparative Study." *Food and Drug Law Journal 55*, no 1, 57-80 (2000).

Chiara, Pier Giorgio. “The IoT and the New EU Cybersecurity Regulatory Landscape.” *International Review of Law, Computers and Technology* 36, no 2 (2022): 1–20. https://doi.org/10.1080/13600869.2022.2060468.

Clark-Ginsberg, Aaron and Rebecca Slayton. “Regulating Risks within Complex Sociotechnical Systems: Evidence from Critical Infrastructure Cybersecurity Standards.” *Science and Public Policy* 46, no 3 (2019): 339–346. https://doi.org/10.1093/scipol/scy061.

Corrales Compagnucci, M., J. Meszaros, T. Minssen, A. Arasilango, T. Ous and M. Rajarajan. “Homomorphic Encryption: The ‘Holy Grail’ for Big Data Analytics and Legal Compliance in the Pharmaceutical and Healthcare Sector?” *European Pharmaceutical Law Review* 3, no 4 (2019): 144–155. https://doi.org/10.21552/eplr/2019/4/5.

Danks, David and Alex John London. “Regulating Autonomous Systems: Beyond Standards.” *IEEE Intelligent Systems* 32, no 1 (2017): 88–91. https://doi.org/10.1109/MIS.2017.1.

Dooley, John F. “Cryptology Before 1500 – A Bit of Magic.” In *History of Cryptography and Cryptanalysis*, 13–23. History of Computing. Cham: Springer International Publishing, 2018. https://doi.org/10.1007/978-3-319-90443-6_2.

Eckhardt, Philipp and Anastasia Kotovskaia. “The EU’s Cybersecurity Framework: The Interplay between the Cyber Resilience Act and the NIS2 Directive.” *International Cybersecurity Law Review* 4 (2023): 147–164. https://doi.org/10.1365/s43439-023-00084-z.

European Commission. *Guidelines on the Qualification and Classification of Stand Alone Software Used in Healthcare within the Regulatory Framework of Medical Devices (MEDDEV) 2.1/6)*. (European Commission, 2016).

Falliere, Nicolas, Liam O. Murchu and Eric Chien. *W32.Stuxnet Dossier*. (Symantec, 2011).

Fosch-Villaronga, Eduard and Christopher Millard. “Cloud Robotics Law and Regulation: Challenges in the Governance of Complex and Dynamic Cyber–Physical Ecosystems.” *Robotics and Autonomous Systems* 119 (2019): 77–91. https://doi.org/10.1016/j.robot.2019.06.003.

Gallese, Chiara. “Legal Issues of the Use of Chatbot Apps for Mental Health Support.” In *Highlights in Practical Applications of Agents, Multi-Agent Systems, and Complex Systems Simulation. The PAAMS Collection*, edited by Alfonso González-Briones, Ana Almeida, Alberto Fernandez, Alia El Bolock, Dalila Durães, Jaume Jordán and Fernando Lopes, 258–267. Communications in Computer and Information Science. Cham: Springer International Publishing, 2022. https://doi.org/10.1007/978-3-031-18697-4_21.

Gerke, Sara, Boris Babic, Theodoros Evgeniou and I. Glenn Cohen. “The Need for a System View to Regulate Artificial Intelligence/Machine Learning-Based Software as Medical Device.” *npj Digital Medicine* 3, no 1 (2020): 53. https://doi.org/10.1038/s41746-020-0262-2.

GOV.UK. “Regulating Medical Devices in the UK.” Last updated July 20, 2023. https://www.gov.uk/guidance/regulating-medical-devices-in-the-uk.

Granlund, Tuomas, Juha Vedenpaa, Vlad Stirbu and Tommi Mikkonen. “On Medical Device Cybersecurity Compliance in EU.” In *2021 IEEE/ACM 3rd International Workshop on Software Engineering for Healthcare (SEH)*, 20–23. Madrid, Spain: IEEE, 2021. https://doi.org/10.1109/SEH52539.2021.00011.

Green, James I. J. “Medical Device Legislation for Custom-Made Devices after the UK Has Left the EU: Answers to Ten Important Questions.” *British Dental Journal* 231, no 8 (2021): 513–521. https://doi.org/10.1038/s41415-021-3530-x.

Han, Ji Eun Diana, Hussein Ibrahim, Olalekan Lee Aiyegbusi, Xiaoxuan Liu, Eliot Marston, Alastair K. Denniston and Melanie J. Calvert. “Opportunities and Risks of UK Medical Device Reform.” *Therapeutic Innovation & Regulatory Science* 56, no 4 (2022): 596–606. https://doi.org/10.1007/s43441-022-00394-0.

Hojnik, Janja. “Technology Neutral EU Law: Digital Goods within the Traditional Goods/Services Distinction.” *International Journal of Law and Information Technology* 25, no 1 (2017): 63–84. https://doi.org/10.1093/ijlit/eaw009.

The Independent Medicines & Medical Devices Safety Review. *First Do No Harm, The Report of the Independent Medicines and Medical Devices Safety Review*. (The Independent Medicines & Medical Devices Safety Review, 2020).

Information Commissioner’s Office. “Privacy-Enhancing Technologies (PETs).” 2022. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies/.

Jimenez, Marco. “Finding the Good in Holmes’s Bad Man.” *Fordham Law Review* 79, no 5 (2011): 2069–2128.

Johnson, Allee. “Closing the Cybersecurity Gap in Medical Devices - Proposing a Safe Harbor System.” *Colorado Technology Law Journal* 20, no 1 (2022).

Johnson, Judith A. “FDA Regulation of Medical Devices.” In *Personalized Medicine and the FDA’s Emerging Role*, edited by Janette Scacco, 75–112. United States: Nova Science Publishers, 2014.

Kamenjašević, Erik and Elisabetta Biasin. “A Commentary on Decentralized Privacy-Preserving Proximity Tracing in the Context of the EU Legal Framework for Medical Devices.” *European Pharmaceutical Law Review* 4, no 2 (2020): 110–114. http://doi.org/10.2139/ssrn.3586418.

Kerckhoffs, Auguste. “La Cryptographie Militaire.” *Journal Des Sciences Militaires* IX (1883): 5–83.

Koops, Bert-Jaap. “Should ICT Regulation Be Technology-Neutral?” In *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners*, edited by Bert-Jaap Koops, Miriam Lips, Corien Prins and Maurice Schellekens. The Hague: T.M.C. Asser Press, 2006. https://doi.org/10.1007/978-90-6704-665-7_4.

Kramer, Daniel B. and Kevin Fu. “Cybersecurity Concerns and Medical Devices: Lessons From a Pacemaker Advisory.” *JAMA* 318, no 21 (2017): 2077. https://doi.org/10.1001/jama.2017.15692.

Kramer, Daniel B., Shuai Xu and Aaron S. Kesselheim. “Regulation of Medical Devices in the United States and European Union.” *The New England Journal of Medicine* (2012): 1–8.

Leal Ghezzi, Tiago and Oly Campos Corleta. “30 Years of Robotic Surgery.” *World Journal of Surgery* 40, no 10 (2016): 2550–2557. https://doi.org/10.1007/s00268-016-3543-9.

Leverett, Eireann, Richar Clayton and Ross Anderson. *Standardisation and Certification of Safety, Security and Privacy in the “Internet of Things*.” (European Commission, 2017). https://doi.org/10.2760/47559.

Leveson, Nancy G. *Safeware: System Safety and Computers*. United States: Addison-Wesley Publishing Company, 1995.

Li, Phoebe, Robin Williams, Stephen Gilbert and Stuart Anderson. “Regulating Artificial Intelligence and Machine Learning-enabled Medical Devices in Europe and the United Kingdom.” *Law, Technology and Humans* 5, no 2 (2023). 94-113. https://doi.org/10.5204/lthj.3073.

Lindstad, Sarita and Kaspar Rosager Ludvigsen. “When Is the Processing of Data from Medical Implants Lawful? The Legal Grounds for Processing Health-Related Personal Data from ICT Implantable Medical Devices for Treatment Purposes under EU Data Protection Law.” *Medical Law Review* 31, no 3 (2022): 317–339. https://doi.org/10.1093/medlaw/fwac038.

Ludvigsen, Kaspar Rosager, Shishir Nagaraja and Angela Daly. “Preventing or Mitigating Adversarial Supply Chain Attacks: A Legal Analysis.” In *Proceedings of the 2022 ACM Workshop on Software Supply Chain Offensive Research and Ecosystem Defenses*, 25–34. Los Angeles: Association for Computing Machinery, 2022. https://doi.org/10.1145/3560835.3564552.

Ludvigsen, Kaspar and Shishir Nagaraja. “Dissecting Liabilities in Adversarial Surgical Robot Failures: A National (Danish) and EU Law Perspective.” *Computer Law & Security Review* 44 (2002): 105656. https://doi.org/10.1016/j.clsr.2022.105656.

Ludvigsen, Kaspar, Shishir Nagaraja and Angela Daly. “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 no 1, 78-93 (2022). https://doi.org/10.1017/err.2021.45.

Lum, John W., Ryan J. Bailey, Victoria Barnes-Lomen, Diana Naranjo, Korey K. Hood, Rayhan A. Lal, Brandon Arbiter, Adam S. Brown, Daniel J. DeSalvo, Jeremy Pettus, Peter Calhoun and Roy W. Beck. “A Real-World Prospective Study of the Safety and Effectiveness of the Loop Open Source Automated Insulin Delivery System.” *Diabetes Technology & Therapeutics* 23, no 5 (2021): 367–375. https://doi.org/10.1089/dia.2020.0535.

Martinetti, Alberto, Peter K. Chemweno, Kostas Nizamis and Eduard Fosch-Villaronga. “Redefining Safety in Light of Human-Robot Interaction: A Critical Review of Current Standards and Regulations.” *Frontiers in Chemical Engineering* 3 (2021): 666237. https://doi.org/10.3389/fceng.2021.666237.

Medical Device Coordination Group. *MDCG 2019-16 Guidance on Cybersecurity for Medical Devices*. (MDCG, 2019). https://ec.europa.eu/docsroom/documents/41863.

Medicines & Healthcare products Regulatory Agency. *Government response to consultation on the future regulation of medical devices in the United Kingdom*. (MHRA, June 26, 2022).

Medina, General Advocate. *Opinion in Case C-588/21* (2023). https://curia.europa.eu/juris/document/document.jsf?docid=274881&doclang=EN

Michalec, Ola, Sveta Milyaeva and Awais Rashid. “When the Future Meets the Past: Can Safety and Cyber Security Coexist in Modern Critical Infrastructures?” *Big Data & Society* 9, no 1 (2022): 205395172211083. https://doi.org/10.1177/20539517221108369.

Ohm, Paul. “The Argument against Technology-Neutral Surveillance Laws.” *Texas Law Review* 88, no 7 (2010): 1685–1713.

O’Sullivan, Shane, Nathalie Nevejans, Colin Allen, Andrew Blyth, Simon Leonard, Ugo Pagallo, Katharina Holzinger, Andreas Holzinger, Mohammed Imran Sajid and Hutan Ashrafian. “Legal, Regulatory, and Ethical Frameworks for Development of Standards in Artificial Intelligence (AI) and Autonomous Robotic Surgery.” *International Journal of Medical Robotics and Computer Assisted Surgery* 15, no 1 (2019): 1–12. https://doi.org/10.1002/rcs.1968.

Phillips, David J. “Privacy Policy and PETs: The Influence of Policy Regimes on the Development and Social Implications of Privacy Enhancing Technologies.” *New Media & Society* 6, no 6 (2004): 691–706. https://doi.org/10.1177/146144804042523.

Palmieri, Sofia and Tom Goffin. “A Blanket That Leaves the Feet Cold: Exploring the AI Act Safety Framework for Medical AI.” *European Journal of Health Law 30*, no 4 (2023): 406-427. https://doi.org/10.1163/15718093-bja10104.

Quamara, Megha, B. B. Gupta and Shingo Yamaguchi. “An End-to-End Security Framework for Smart Healthcare Information Sharing against Botnet-based Cyber-Attacks.” 2021 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 2021. https://ieeexplore.ieee.org/document/9427753/.

Quigley, Muireann and Downey, Laura. “Living in a Material World? Regulatory Challenges of Software as a Medical Device.” Unpublished journal article.

Quigley, Muireann, Laura Downey and Jean McHale. “The Future of Medical Devices Regulation in the United Kingdom? Brexit and Beyond.” *Law, Technology and Humans* 5, no 2 (2023): 21-42. https://doi.org/10.5204/lthj.3102.

Reed, Chris. "Taking Sides on Technology Neutrality." *SCRIPT-Ed* 4, no 3 (2007): 263–284. https://doi.org/10.2966/scrip.040307.263.

Roberts, Joseph T. F., Victoria Moore and Muireann Quigley. "Prescribing Unapproved Medical Devices? The Case of DIY Artificial Pancreas Systems." *Medical Law International* 21, no 1 (2021): 42–68. https://doi.org/10.1177/0968533221997510.

Roth, Vincent J. "How Much FDA Medical Device Regulation Is Required?" *North Carolina Journal of Law & Technology* 15, no 3 (2014).

Teece, David J. "Profiting from Innovation in the Digital Economy: Enabling Technologies, Standards, and Licensing Models in the Wireless World." *Research Policy* 47, no 8 (October 2018): 1367–1387. https://doi.org/10.1016/j.respol.2017.01.015.

Tschider, Charlotte A. "Deus Ex Machina: Regulating Cybersecurity and Artificial Intelligence for Patients of the Future." *Savannah Law Review* 5, no 1 (2017): 177–210.

Tschider, Charlotte A. "Medical Device Artificial Intelligence: The New Tort Frontier." *Brigham Young University Law Review* 46, no 6 (2021): 1551–1617.

Tschider, Charlotte. "Prescribing Exploitation." *Maryland Law Review* 82, no 4 (2023): 857–919. https://digitalcommons.law.umaryland.edu/mlr/vol82/iss4/2.

Twining, William. "The Bad Man Revisited." *Cornell Law Review* (1972): 39–67. https://doi.org/10.4324/9781315086323-3.

Schmitz, Sandra. "Conceptualising the Legal Notion of 'State of the Art' in the Context of IT Security." In *Privacy and Identity Management. Between Data Protection and Security*, edited by Michael Friedewald, Stephan Krenn, Ina Schiering and Stefan Schiffner25–32. IFIP Advances in Information and Communication Technology. Cham: Springer International Publishing, 2022. https://doi.org/10.1007/978-3-030-99100-5_3.

Schmitz-Berndt, Sandra. "Don't Tell Them Now (or at all) – Responsible Disclosure of Security Incidents under NIS Directive and GDPR." *International Review of Law, Computers & Technology* 35, no 2 (2021): 101–115. https://doi.org/10.1080/13600869.2021.1885103.

Strielkina, Anastasiia, Oleg Illiashenko, Marina Zhydenko and Dmytro Uzun. "Cybersecurity of Healthcare IoT-Based Systems: Regulation and Case-Oriented Assessment." In *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, 67–73. Kyiv: IEEE, 2018. https://doi.org/10.1109/DESSERT.2018.8409101.

US Food and Drug Administration. *Changes to Existing Medical Software Policies Resulting from Section 3060 of the 21st Century Cures Act: Guidance for Industry and Food and Drug Administration Staff.* (FDA, September 2019).

US Food and Drug Administration. *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions: Guidance for Industry and Food and Drug Administration Staff.* (FDA, September 27, 2023).

US Food and Drug Administration. "How to Determine if Your Product is a Medical Device. FDA." Last updated September 29, 2022. https://www.fda.gov/medical-devices/classify-your-medical-device/how-determine-if-your-product-medical-device.

US Food and Drug Administration. *Policy for Device Software Functions and Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff.* (FDA, September 28, 2022).

US Food and Drug Administration. "Product Classification." FDA. Last updated October 30, 2023. https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfPCD/classification.cfm.

Wallis, Tania and Chris Johnson. "Implementing the NIS Directive, Driving Cybersecurity Improvements for Essential Services." 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, Ireland, 2020. https://doi.org/10.1109/CyberSA49311.2020.9139641.

Xenofontos, Christos, Ioannis Zografopoulos, Charalambos Konstantinou, Alireza Jolfaei, Muhammad Khurram Khan and Kim-Kwang Raymond Choo. "Consumer, Commercial, and Industrial IoT (In)Security: Attack Taxonomy and Case Studies." *IEEE Internet of Things Journal* 9, no 1 (2022): 199–221. https://doi.org/10.1109/JIOT.2021.3079916.

Zuckerman, Diana M., Paul Brown and Steven E. Nissen. "Medical Device Recalls and the FDA Approval Process." *Archives of Internal Medicine* 171, no 11 (2011): 1006–1011. https://doi.org/10.1001/archinternmed.2011.30.

Primary Legal Material

European Union

Agreement on the Withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community [2019] OJ C 384 I/01.

Case C-255/02, *Halifax plc and Others v. HM Customs & Excise*, 2006 EU:C:2006:121.

Council Directive 93/42/EEC of 14 June 1993 Concerning Medical Devices [1993] OJ L169/1.

Directive (EU) 2016/745 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union [2016] OJ L194/1.

Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 Establishing the European Electronic Communications Code [2018] OJ LL321/36.

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity Across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive) [2022] OJ L333/80.

Joined Cases C-59/13 and C-58/13, *Angelo Alberto Torresi and Pierfrancesco Torresi v. Consiglio dell'Ordine degli Avvocati di Macerata*, 2014 ECLI:EU:C:2014:2088.

Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM (2021) 206 final, 2021/0106 (COD).

Proposal for a Regulation of the European Parliament and of the Council Laying Down Measures to Strengthen Solidarity and Capacities in the Union to Detect, Prepare for and Respond to Cybersecurity Threats and Incidents COM (2023) 209 final, 2023/0109 (COD).

Proposal for a Regulation of the European Parliament and of the Council on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulation (EU) 2019/1020 COM (2022) 454 final, 2022/0272 (COD).

Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space COM (2022) 197/2, 2022/0104 (COD).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L1191.

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 L117/1.

Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on In Vitro Diagnostic Medical Devices and Repealing Directive 98/79/EC and Commission Decision 2010/227/EU [2017] OJ L117/176.

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [2019] OJ L151/15.

United States

6 U.S.C.

18 U.S.C.

21 U.S.C.

Consolidated Appropriations Act 2022, Pub. L. No. 117-103, 136 Stat. 49 (2022)

United Kingdom

Medical Devices Regulations 2002

Medical Devices (Amendment etc.) (EU Exit) Regulations 2020