Volume **5** (2) 2023 https://doi.org/10.5204/lthj.3068

New Cybersecurity Requirements for Medical Devices in the EU: The Forthcoming European Health Data Space, Data Act, and Artificial Intelligence Act

Elisabetta Biasin
KU Leuven, Belgium
Burcu Yaşar
University of Hamburg, Germany
Erik Kamenjašević
KU Leuven, Belgium

Abstract

The regulation of cybersecurity for medical devices keeps evolving in the European Union (EU). In the past few years, new pieces of legislation have been added to the initial framework for medical device cybersecurity, including the Medical Device Regulation, the General Data Protection Regulation and the Cybersecurity Act. The Artificial Intelligence Act, the European Health Data Space Regulation and the Data Act are forthcoming laws that contain cybersecurity-related requirements applicable to medical devices. This article examines the requirements stemming from each of these, as well as their role vis-a-vis the existing legal framework. We observe that despite being comprehensive and wide ranging in their changes, these new regulations may be inadequate for the task of ensuring the cybersecurity of medical devices. In our view, this approach by the EU legislature is inadequate because it fails to foresee cybersecurity requirements in a way that is truly linked with the already existing cybersecurity laws. To help address this problem, the article offers a set of workable recommendations that EU legislators would be well advised to take on board in respect of specific regulations, as well as in general, when establishing cybersecurity-related requirements.

Keywords: Medical device; cybersecurity; artificial intelligence; MDR; EHDS Regulation.

1. Introduction

In recent years, the healthcare sector has undergone a digital transformation due to medical devices that rely on network connectivity and advanced technologies. These advances bring numerous benefits to patients; however, they also present significant cybersecurity challenges that ought to be addressed. Interconnected medical devices, ranging from implantable cardiac devices to insulin pumps, are susceptible to various cybersecurity threats, including unauthorised access, data breaches and medical device functionality manipulation. A successful cyber-attack on a medical device could have severe consequences, such as compromising patient privacy and eroding trust in the healthcare system, not to mention directly harming patients' health.[1] In the European Union (EU), where the rights to health and data protection are fundamental principles, the cybersecurity of medical devices has become a critical concern for lawmakers, policymakers, healthcare providers and medical device manufacturers.

[1] See, e.g., Fuster, "Cybersecurity Regulation;" Papakonstantinou, "Cybersecurity as Praxis;" Chiara, "The IoT and EU Cybersecurity;" "Biasin, "Regulatory Challenges;" Biasin, "New Challenges."

Much has been written on cybersecurity generally and on medical device cybersecurity more specifically; however, the latter is a matter of relatively recent regulation in the EU. In some of our previous work,[2] we set out the existing legal framework on cybersecurity, noting that this framework consists of sector-specific cybersecurity-related requirements (set by the EU Medical Device Regulation [MDR])[3] and other horizontal (applying across different sectors) cybersecurity legislation (e.g., directives on the security of network and information systems (NIS)[4] and the Cybersecurity Act [CSA]).[5, 6] However, even more recently, three new legislative proposals – the Artificial Intelligence (AI) Act, the European Health Data Space (EHDS) proposed regulation and Data Act – have been introduced that would add to the cybersecurity requirements relevant to medical devices.[7]

Few studies in the legal literature have analysed the potential effects of these pending legislative reforms on medical device cybersecurity or examined the challenges they could create from a legal standpoint. In this context, this article examines some of the understudied legal challenges that the forthcoming legislation may bring to medical device cybersecurity in the EU. To do so, in section two, we examine both the current and forthcoming EU laws applicable to medical device cybersecurity. This is followed, in section three, by a look at currently available interpretative guidance issued at the EU level about medical device cybersecurity. In section four, we outline some significant legal challenges stemming from the new legislative proposals (i.e., the AI Act, the EHDS Regulation and the Data Act). This examination reveals an incoherent approach of the EU legislature in relation to new cybersecurity-related requirements. In section five, we make recommendations to the EU lawmakers to help address these challenges, not only in relation to the aforementioned proposals, but also in relation to the drafting of future cybersecurity-related provisions more generally.

2. Legal Framework for the Cybersecurity of Medical Devices

2.1 Existing Legislation

To give an idea of the already complicated legal landscape in the EU regarding the cybersecurity of medical devices, this sub-section provides a brief overview of some of the most important and relevant pieces of legislation. In the EU, security risks are addressed by various laws that specifically focus on data, cybersecurity, AI and/or sector-specific rules (including those specific to the healthcare sector). For illustrative purposes, we choose to briefly comment on three general categories of legislation.

The first category we consider as relevant is *Medical Device Laws*, which encompasses the Medical Devices Regulation (MDR) and the In Vitro Diagnostic Medical Devices Regulation (IVDR).[8] The second category is *Cybersecurity Laws*, which includes the NIS Directive – replaced by the so-called Network Information System 2.0 (NIS2) Directive – and the CSA. The third category relates to *Data Laws*, which includes the General Data Protection Regulation (GDPR)[9] and the Data Governance Act (DGA).[10] As Figure 1 illustrates, these are overlapping areas of law, all with implications for each other.

[2] Biasin, "Regulatory Challenges."
[3] 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 (Medical Device Regulation or MDR).
[4] Directive (EU) 2016/1148 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 (NIS Directive); 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).
[5] 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).
[6] Biasin, "New Challenges."
[7] Proposal for a Regulation of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data (Data Act), COM/2022/68 final; Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, COM/2022/197 final; Proposal for a 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.
[8] 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. This manuscript leaves out the IVDR for reasons of space and focuses only on the MDR.
[9] 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 (GDPR).
[10] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data Governance and Amending Regulation (EU) 2018/1724 (Data Governance Act) [2018] OJ L152/1.

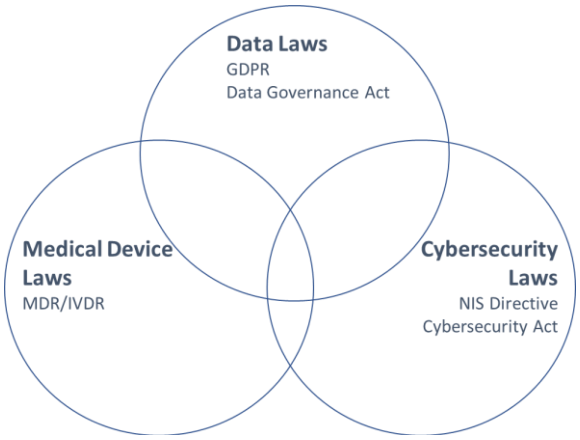

Figure 1. Current EU Legal Framework for the Cybersecurity of Medical Devices

We start our illustration of the medical devices' cybersecurity legal framework with Medical Device Laws. The MDR is the primary law governing medical devices. It sets essential safety and performance requirements that medical device manufacturers must adhere to before putting their devices on the market. These safety and performance requirements, relevant from a cybersecurity perspective, are supplemented by the Medical Device Coordination Group (MDCG) – a body established by the same MDR to provide guidance on the regulation of this sector.[11] In its guidance, the MDCG identified and summarised all the pre-market and post-market requirements that arise across the life cycle of medical devices according to the MDR. We have written a detailed report on these requirements elsewhere.[12] In a nutshell, the requirements in the MDR that are relevant from a cybersecurity perspective include the adoption of a risk-management system, the execution of a risk assessment, software interaction with the information technology (IT) environment (including interoperability and compatibility), IT security measures (including protection against unauthorised access) and reporting for serious cyber incidents.

The second category we examine is Cybersecurity Laws, in which we include the NIS2 Directive and the CSA.[13] The former is the primary law that comprehensively addresses cybersecurity across the EU Member States. As an EU Directive, it lays down general rules that have to be transposed by the Member States into national legislation to achieve a common level of cybersecurity across the EU.[14] The NIS2 Directive sets out cybersecurity risk-management measures and reporting obligations for the entities in its scope (i.e., the essential and important entities). These entities are required to take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of NIS that they use for their service provisions and to prevent or minimise the impact of incidents.[15] The Directive applies to a variety of different sectors. Medical device manufacturers are considered in the scope of the Directive, as they could qualify, in principle, as essential or important entities.[16] The latter law, the CSA, sets out requirements for the voluntary cybersecurity certification of information communications technology (ICT) products, including medical devices.

The third category we look at is Data Law, in which we include the GDPR and the Data Governance Act (DGA). The GDPR contains rules for the secure processing of personal data that establish the principle of integrity and confidentiality of data processing. As part of its security requirements, the GDPR requires the adoption of technical and organisational measures to ensure a level of security appropriate to the risk.[17] When there is a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data, the GDPR requires to notify a 'personal data breach'. When such a breach is likely to result in a risk to the rights and freedoms of natural persons, it is necessary to notify the supervisory authority and the affected data subjects.[18] As to the second item in this category, the Data Governance Act's

[11] Medical Device Coordination Group (MDCG), "MDCG 2019-16."
[12] For a broader description and comment, see Biasin, "Regulatory Challenges."
[13] For more information on the NIS2 and CSA, see Ludvigsen, "The Role of Cybersecurity."
[14] The Member States are required to transpose the Directive by 17 October 2024.
[15] See NIS2 Directive, supra note 4, art. 21.
[16] See NIS2 Directive, supra note 4, art. 3 and Annex II, Other Critical Sectors, Sector n. 5 "Manufacturing," which includes "Manufacture of medical devices and *in vitro* diagnostic medical devices."
[17] GDPR, supra note 9, art. 32.
[18] GDPR, supra note 9, arts. 33–35.

general objective is to set out rules on the re-use of certain categories of data by public sector bodies in the EU. Importantly, this regulationct establishes 'secure processing environments', which we will analyse in the sections below.[19]

2.2 Forthcoming Legislation Concerning the Cybersecurity of Medical Devices

Three forthcoming proposals (i.e., the AI Act, the EHDS and the Data Act proposals) will soon reshape the already complicated legal framework for the cybersecurity of medical devices in significant ways. In this sub-section, we provide an overview of these proposals that will add to the above-described legal framework.

The first general observation to be made about these legislative proposals is that they are an important step towards increased harmonisation across different EU Member States, as they will be regulations that once adopted will be directly applicable in all EU Members States without the need for implementation through domestic law. The second general observation is that the main purposes and focuses of these legislative initiatives vary considerably (e.g., data sharing, the availability of health data and AI-specific legislation). Nevertheless, they all contain cybersecurity-relevant provisions concerning medical devices that should be diligently distilled.

Put forward by the European Commission in April 2021 as a result of year-long policy discussions, the AI Act proposal aims to address the gaps in the existing legislation to adequately address the needs of the digitalising world. The AI Act proposal aims to regulate various aspects of AI; however, the AI Act proposal is of high relevance for broader cybersecurity law and policy, as it establishes a cybersecurity requirement for high-risk AI systems (as discussed further in section three). However, the AI Act proposal has certain shortcomings in relation to its alignment with the existing legislation, the understanding of cybersecurity contained within it and the adequacy of its provisions for protecting patients. These shortcomings, along with some recommendations, are discussed in section three.

The Data Act proposal is a cross-sector regulation laying down rules on data sharing between businesses, businesses and consumers, and from businesses to governments. The business-to-consumer and business-to-business rules foresee the obligation to make data generated by the use of products or related services accessible so that data are, by default, easily, securely and directly accessible by the user.[20] The business-to-government data sharing rules foresee the obligation to make data available from data holders to public sector bodies or union institutions, agencies or bodies where there is an exceptional need to perform a task in the public interest. The Data Act proposal is deemed to apply to medical devices,[21] and from the cybersecurity side, the most relevant provisions are those setting out data-sharing obligations for the government in the case of a public emergency.[22]

The EHDS Regulation was issued by the European Commission in April 2022. The proposal has the objective of promoting the primary and secondary use of health data (which encompasses both personal and non-personal electronic health data),[23] strengthening the rights of natural persons regarding the availability and control of their electronic health data and laying down safety requirements (including cybersecurity) for the placing on the market of electronic health records (EHR) systems. The cybersecurity requirements include access management rights for healthcare practitioners, logging mechanisms, the monitoring of the origins and categories of electronic health data, and identification mechanisms.[24] In addition, the EHDS proposal includes cybersecurity-related provisions to ensure the sharing of electronic health data within a 'secure processing environment'.[25] As

[19] The "secure processing environment" is defined by the DGA, supra note 10, art. 2(14). According to this definition, it consists of "the physical or virtual environment and organisational means to ensure compliance with Union law, such as Regulation (EU) 2016/679, in particular with regard to data subjects' rights, intellectual property rights, and commercial and statistical confidentiality, integrity and accessibility, as well as with applicable national law, and to allow the entity providing the secure processing environment to determine and supervise all data processing actions, including the display, storage, download and export of data and the calculation of derivative data through computational algorithms."

[20] See Data Act proposal, supra note 7, chs. II–III.

[21] See Data Act proposal, supra note 7, rec. 14: "Physical products that obtain, generate or collect, by means of their components, data concerning their performance, use or environment and that are able to communicate that data via a publicly available electronic communications service (often referred to as the Internet of Things) should be covered by this Regulation. (…) Such products may include vehicles, home equipment and consumer goods, medical and health devices or agricultural and industrial machinery."

[22] See Data Act proposal, supra note 7, ch. V.

[23] Personal electronic data are defined as: "data concerning health and genetic data as defined in Regulation (EU) 2016/679, as well as data referring to determinants of health, or data processed in relation to the provision of healthcare services, processed in an electronic form" (EHDS proposal, art. 2(2)(a)). Non-personal electronic health data refers to "data concerning health and genetic data in electronic format that falls outside the definition of personal data provided in Article 4(1) of Regulation (EU) 2016/679" (EHDS proposal, art. 2(2)b)).

[24] EHDS proposal, supra note 7, Annex II.

[25] EHDS proposal, supra note 7, art. 50.

the following sections demonstrate, the EHDS proposal might apply to medical devices if they fall under the definition of an EHR system.[26]

To support the description and general collocation of the laws given here and to help better understand the relationship between them, let us return to our graphical representation of the medical device cybersecurity framework (Figure 1). We can now add the EHDS proposal and the Data Act to the Data Laws category. We also propose a new category of AI Laws for the AI Act proposal (Figure 2). We now turn to examine each of the forthcoming proposals in more depth, and we focus on the shortcomings and challenges that each of them face in respect of medical devices' cybersecurity.

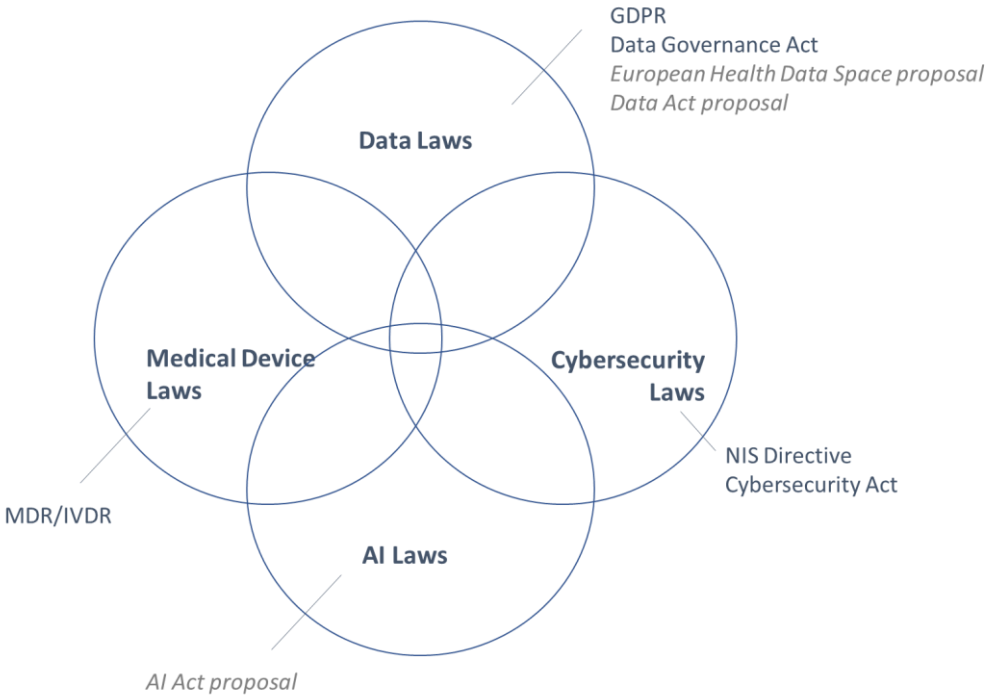

Figure 2. Prospective EU Legal Framework for the Cybersecurity of Medical Devices

3. The New Cybersecurity Requirements in the Forthcoming AI Law

3.1 The AI Act (also) as a Cybersecurity Legislation

The EU's AI Act proposal is a result of years-long policy initiatives and discussions that demonstrate that the existing legislation may need to be complemented by some AI-specific rules and requirements. The existing legislation prescribes requirements for the health and safety of individuals and applies to AI systems, nevertheless fears have been raised that the emerging or intensified features of new technologies, such as connectivity and autonomy, will make these requirements insufficient.[27] For instance, as the concepts of safety and cybersecurity are related but distinct,[28] there are concerns over the suitability of safety rules to regulate cybersecurity issues. As a result, the proposal for the AI Act was introduced by the European Commission in April 2021 and it is currently discussed by the EU decision makers at the time of the writing. Once in force, the AI Act has the potential to affect any medical device manufacturer in the world if they wish to provide their products to the EU market.[29]

[26] EHR system means "any appliance or software intended by the manufacturer to be used for storing, intermediating, importing, exporting, converting, editing or viewing electronic health records" (art. 2(2)(n) EHDS proposal). Its relevance to medical devices will be explained further in section 4.
[27] European Commission, Report on the Safety and Liability Implications of Artificial Intelligence, the Internet of Things and Robotics, 19 February 2020, COM (2020) 64 final.
[28] Vedder, "Safety, Security and Ethics."
[29] AI Act proposal, supra note 7, Explanatory Memorandum, 2.

The AI Act proposal is underpinned by a risk-based approach that allows regulatory intervention to the extent that it is necessary to address a variety of risks.[30] In this section, we briefly look into different risk categories established by the proposal. We then examine whether and how the AI Act proposal can be perceived as (also) cybersecurity legislation, as well as looking at the specifics and limitations of the way in which it regulates cybersecurity.

3.2 Scope of Application

The AI Act proposal establishes rules for three risk categories: unacceptable, high-risk and limited risk. Unacceptable risk AI is any AI designed through the prohibited AI practices as defined in Article 5 (e.g., subliminal techniques) and shall not be placed on the market or put into service due to the heightened risks to fundamental rights. Limited risk AI (or AI with transparency obligations) includes certain applications, such as chatbox or deepfakes.[31] High-risk AI, defined in Article 6, constitutes the main focus of the AI Act proposal and includes medical device software (as discussed below). High-risk AI systems are allowed on the market provided that they fulfil the relevant requirements set out by the AI Act, including those relating to cybersecurity. All other AI systems, which fall outside the scope of these three categories, constitute minimal or low-risk AI and are not been subject to any mandatory requirements under the AI Act but are encouraged to voluntarily adhere to the high-risk AI requirements.

The AI Act proposal defines high-risk AI with reference to (i) some products covered by existing EU safety legislation or (ii) systems intended to be used for certain purposes.[32] Medical devices fall into the first definition. According to this definition, high-risk AI comprises systems developed by a wide variety of computational techniques and approaches[33] that (i) constitute a product or a safety component of a product covered by the EU safety legislation listed in Annex II of the AI Act, and (ii) need a conformity assessment as part of that legislation.[34] Most AI medical device software is expected to be a high-risk AI because most will fall under the legislation covered by the AI Act (i.e., the EU MDR or IVDR) and will require a third-party conformity assessment under the relevant legislation.

To constitute high-risk AI, it is, therefore, first and foremost necessary that the software constitutes a 'medical device' as defined in the MDR or IVDR. Essential to the definition of a medical device is that the manufacturer must intend the device to have a medical purpose as set out in the legislation.[35] This paper will not analyse the scope of application of the AI Act proposal for the products that are not intended for medical purposes (generally known as lifestyle and wellness applications), as it specifically focuses on those products that are uncontrovertibly medical devices. However, we do discuss the element of intention required in the definition of 'medical device' in section four (in relation to the EHDS proposal).

3.3 Cybersecurity Shortcomings

The AI Act proposal sets out common requirements for high-risk AI systems and prohibits certain AI practices, and in that sense, is not strictly a cybersecurity-specific law. However, it often refers to cybersecurity and establishes an obligation of cybersecurity for high-risk AI systems.[36] Moreover, Recital 5a (which is not a binding part of the legislation but helps to interpret the main text) specifies that it is necessary to address 'cybersecurity concerns' to ensure that AI systems are in line with EU values.[37] It is, therefore, clear that the EU legislature intends to make the AI Act a part of the EU law that regulates cybersecurity in the context of certain technologies. This includes medical device software. Nevertheless, despite containing significant provisions relating to the cybersecurity of high-risk AI systems, the AI Act proposal does not provide a definition of cybersecurity. What follows is a brief overview of the understanding of the term in the wider EU context to better understand the AI Act's approach to cybersecurity. We then examine the cybersecurity provision of the AI Act proposal.

As established in section 2.1, cybersecurity is a developing area in the EU with a patchwork of legislation and policies, which continues to grow. A myriad of definitional approaches to cybersecurity have been observed; however, Article 2(1) of the

[30] AI Act proposal, supra note 7, 3. There it states that the regulation "… puts in place a proportionate regulatory system centred on a well-defined risk-based regulatory approach that does not create unnecessary restrictions to trade, whereby legal intervention is tailored to those concrete situations where there is a justified cause for concern or where such concern can reasonably be anticipated in the near future."
[31] AI Act proposal, supra note 7, Explanatory Memorandum, 52.
[32] AI Act proposal, supra note 7, art. 6(1).
[33] AI Act proposal, supra note 7, Annex I.
[34] AI Act proposal, supra note 7, art. 6(1).
[35] To qualify as a medical device (a product of the listed legislation in Annex II) in the first place, the technology should be a product intended by the manufacturer to be used for a medical purpose. The intention of the manufacturer remains a significant constitutive element that determines the nature of the device. This intention can be observed, for instance, in marketing strategies and disclaimers.
[36] AI Act proposal, supra note 7, art. 15.
[37] European Parliament, Draft Compromise Amendments on the Draft Report, 16 May 2023, Recital 5a.

Cybersecurity Act constitutes the main formal definition of cybersecurity in the EU law.[38] As cybersecurity is a multi-faceted issue subject to the consideration of a wide range of policy areas, there is no common understanding of the concept.[39] The conceptual approaches reflect a spectrum that on the one hand, defines cybersecurity very narrowly to reduce it to solely a technical matter[40] but on the other hand, is a very broad concept regulated by an integrated approach at the crossroads of a multitude of policies and regulatory aspects.[41] The first extreme runs the risk of ignoring the human and societal aspects or not duly protecting the rights of legal or natural persons (i.e., the actual beneficiaries of the cybersecurity regime).[42] The second extreme runs the risk of being 'overly inclusive' to a level that can override regulatory efforts.[43]

In the face of the myriad of definitional approaches, a distinction between two main types of cybersecurity has been suggested in the literature: *cybersecurity as a praxis* and *cybersecurity as a state*.[44] Cybersecurity as a praxis refers to 'all actions and measures' necessary to achieve a variety of aims of cybersecurity policies.[45] This concept emphasises the process in which various cybersecurity actors, such as service providers, developers and security experts, are tasked with implementing a wide range of security measures appropriate to the security risks. These measures could include purely technical means and organisational arrangements, such as establishing institutional roles to make relevant decisions.[46] Cybersecurity as a state understands cybersecurity as a 'protective sphere' or 'sphere of protection', where individuals, public entities or private entities 'may enjoy a state of cybersecurity'.[47] The state of being secure is dependent on the first type of cybersecurity in the sense that all necessary 'actions and measures' need to be taken as part of a cybersecurity process to establish an area of protection where all persons can expect to be secure or protected from any interferences to their security.[48] This distinction is important because it shows that cybersecurity is not only about the protection of information systems (since these systems are not the main recipients[49] of cybersecurity) but is also about the protection of those who are entitled to rights and claims to enjoy security and related rights. Article 2(1) of the Cybersecurity Act embeds both of these understandings of cybersecurity, as it defines cybersecurity as 'the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats'.[50] As we argue further in the next section, this understanding of cybersecurity should be operative in the cybersecurity requirement enshrined by Article 15 of the AI Act proposal.

Regrettably, the AI Act does not refer to the definition of cybersecurity under the Cybersecurity Act. However, Article 42(2) of the AI Act proposal does refer to the Cybersecurity Act with regard to compliance. This Article states that high-risk AI systems that have a (voluntary) certification or a statement of conformity in accordance with the Cybersecurity Act shall be presumed to be in compliance with the cybersecurity requirements of the AI Act to the extent that the certification or statement partially or fully overlaps with these requirements. Given this, it is at least arguable that the definition of the Cybersecurity Act may nonetheless bind medical device software if it goes through the so-called voluntary certification mechanism. This case is strengthened by the fact that the definition – as within the Cybersecurity Act – is adopted by other recently revised cybersecurity legislation.[51]

Having a commonly agreed definition of cybersecurity is an important step forward and will help ensure a consistent application of the term throughout EU law. The explicit adoption (as opposed to the current implicit adoption) of this definition in the AI Act proposal would contribute to regulatory consistency and to clarifying the meaning of the term for the AI providers and users.[52]

[38] Papakonstantinou, "Cybersecurity as Praxis," 3–4. Article 2(1) of the CSA defines "cybersecurity" as "the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats."
[39] Fuster, "Cybersecurity Regulation," 102–104.
[40] Fuster, "Cybersecurity Regulation," 107.
[41] Fuster, "Cybersecurity Regulation," 102–104.
[42] Papakonstantinou, "Cybersecurity as Praxis," 5.
[43] Fuster, "Cybersecurity Regulation," 112.
[44] Papakonstantinou, "Cybersecurity as Praxis."
[45] Papakonstantinou, "Cybersecurity as Praxis," 4.
[46] Papakonstantinou, "Cybersecurity as Praxis," 4.
[47] Papakonstantinou, "Cybersecurity as Praxis," 4.
[48] Papakonstantinou, "Cybersecurity as Praxis," 6.
[49] Papakonstantinou, "Cybersecurity as Praxis," 5.
[50] See Cybersecurity Act, supra note 5, art. 2(1). This definition is the main legislative definition of cybersecurity in the EU. See Papakonstantinou, "Cybersecurity as Praxis," 3–4.
[51] NIS2 Directive, supra note 4, art. 6(3).
[52] See Biasin, "New Challenges," 55–56. They followed this line of argumentation in relation with the EU soft-law guidance on medical device cybersecurity (i.e., the MDCG, "MDCG 2019-16").

3.4 Article 15 of the AI Act Proposal

Article 15 of the AI Act proposal establishes, among other things, a cybersecurity requirement for high-risk AI systems. Under the first paragraph, the high-risk AI systems (and thus medical device software) *'*shall be designed and developed in such a way that they achieve, in light of their intended purpose, an appropriate level of accuracy, robustness and cybersecurity and perform consistently in those respects throughout their lifecycle'. As per Article 15(4) of the AI Act proposal, medical device software shall be resilient as regards any attempts by unauthorised third parties to alter their use or performance by exploiting the system vulnerabilities. The same Article establishes that the technical solutions to address AI-specific vulnerabilities shall include, where appropriate, measures to prevent data poisoning, adversarial examples or model flaws.

The meaning of *cybersecurity as a praxis* can be understood by reference to these 'technical solutions'. AI providers must determine which technical solutions would be appropriate to the relevant circumstances and risks to ensure the cybersecurity of AI systems and implement them accordingly. These solutions are not provided in a non-exhaustive manner, as it is left to the designers and developers to tailor them depending on the level of risks, circumstances and the intended purpose. Conversely, an understanding of *cybersecurity as a state* can be deduced from the wording, '[high-risk AI systems] achieve ... an appropriate level of ... cybersecurity', '[h]igh-risk AI systems shall be resilient' and '[t]he technical solutions aimed at ensuring the cybersecurity of high-risk AI systems'.[53] Thus, the *technical solutions* implemented by medical software providers should be suitable to achieve a *state of cybersecurity* where patients and other stakeholders can enjoy their rights and interests. These cybersecurity requirements should be read as an 'obligation of result', which is a stricter form of liability than an 'obligation of best efforts', as the former requires providers to achieve a certain result (i.e., the state of cybersecurity) and does not see it as sufficient that the provider shows that they have engaged in best efforts if this result is not achieved.[54]

Two main limitations can be observed regarding Article 15 of the AI Act proposal. The first limitation is that the proposal's 'state of cybersecurity' only grants this state of protection to high-risk AI systems (i.e., software or intelligent computer systems). The AI Act proposal does not create an explicit link between cybersecurity and the actual beneficiaries of cybersecurity (i.e., cybersecurity as a state where individuals and legal entities enjoy rights in an area of protection). This limitation could be addressed by adopting the definition of cybersecurity set out in the Cybersecurity Act.[55] The second and related limitation is that Article 15 refers only to 'technical solutions' to ensure cybersecurity and omits organisational measures. Orlando and Dewitte argue that the cybersecurity domain's interdisciplinary nature makes it dependent on the collaboration of professionals from different disciplines, including developers and lawyers.[56] Such collaboration is enabled by organisational measures, such as impact assessments,[57] institutional roles or complaint procedures. These organisational measures are essential to fulfil cybersecurity goals and ensure the effective enjoyment of the rights of the right-holders. The organisational measures are not new to cybersecurity law since they are referred to in other EU cybersecurity legislation as outlined in section two above; for instance, the NIS2 Directive enumerates organisational measures as part of risk-management measures, such as the establishment of policies on risk analysis, training, assessment procedures and measures for supply chain security.[58]

To a certain extent, some GDPR provisions – which can be considered a counterpart to Article 15 of the AI Act proposal – may provide useful insights for the legislature and could be used when considering the structure of the cybersecurity provisions in Article 15 of the AI Act. The two most relevant Articles in the GDPR are: (1) Article 25(1) on data protection by design and by default, and (2) Article 32 on the security of personal data. These establish obligations for data controllers to implement both technical and organisational measures. These measures must be tailored to effectively implement the related data protection principles, including data security,[59] and they must 'integrate the necessary safeguards … to the rights of data subjects'.[60] To determine which exact measures must be implemented, the GDPR obliges data controllers to take into account certain factors: the state of the art; the costs of implementation; the nature, scope, context and purposes of the processing; and the risk of varying likelihood and severity for the rights and freedoms of natural persons. The GDPR's model thus makes a

[53] AI Act proposal, supra note 7, arts. 15(1), 15(4).
[54] The distinction between the obligation of result and the obligation of best efforts can be found in civil law. See Zanfir, "Tracing the Right," 236. A result of the obligation can also be found in the GDPR's data protection by design requirement. See Jasmontaite, "Data Protection by Design," 174.
[55] See Cybersecurity Act, supra note 5, art. 2(1).
[56] Orlando, "The 'By Design' Turn," 247–248.
[57] Orlando, "The 'By Design' Turn," 247–248.
[58] NIS2 Directive, supra note 4, art. 21.
[59] In our view, Data Protection by Design and by Default (DPbDD), set out in Article 25, encompasses security-by-design. See also Bygrave, "Security by Design," 141–142.
[60] GDPR, supra note 9, art. 25(1).

clear link between the technology design stage and the organisational measures to better integrate cybersecurity issues into the institutional structure and the protection of individuals. This model also provides more explicit guidance in the determination of the appropriateness of certain measures, as it provides a set of clear factors that show exactly what is at stake.

The GDPR model could serve for strengthening the cybersecurity provisions of the AI Act proposal. In its current form, the AI Act proposal lacks a clear definition of cybersecurity and hence a clear link between cybersecurity and the protection of individual rights. This limitation is exacerbated by the fact that the AI Act restricts the measures to address cybersecurity to technical measures, reducing the measures to a narrowly defined technical matter. We therefore recommend (i) adopting the definition of cybersecurity in the Cybersecurity Act, as this would contribute to the consistent application of the term and increase the regulatory clarity as to the actual beneficiaries of cybersecurity, and (ii) explicitly including organisational measures as part of cybersecurity measures and factors that must be taken into account in the determination of such measures. We believe that the GDPR's data protection model is insightful in this respect. Adopting these recommendations is especially important, as the GDPR does not apply to the processing of non-personal data, and thus the security of the software could be dependent on the AI Act provisions. This would be the case if non-personal data, for instance, anonymised data, as we discuss in the context of EHDS proposal below, is processed. The next section will discuss how the security requirements could be further strengthened.

4. The New Cybersecurity Requirements in the Forthcoming Data Laws

In this section, we illustrate how Data Laws apply to medical devices, and how their cybersecurity-related requirements intersect with Cybersecurity Laws within the medical device cybersecurity legal framework.

4.1 Cybersecurity of EHR Systems

Let us begin with the EHDS proposed Regulation. It is our contention that the EHDS proposal is relevant to the medical device cybersecurity legal framework because (a) it may introduce novel cybersecurity requirements for medical devices that are considered EHR systems, and (b) it prescribes security requirements on health data sharing that may also concern medical devices. In this section, we analyse the first aspect(letter (a)), and in the next section, we analyse the second part of this contention (letter (b)), scrutinising the possible legal challenges in relation to both. We start then with the introduction by the EHDS proposal of cybersecurity requirements for medical devices that are considered EHR systems, looking first at how a medical device may qualify as an EHR system, before turning to the cybersecurity requirements (and the practical consequences of these requirements) that the EHDS proposal introduces for EHR systems.

The EHDS proposal might apply to medical devices if they fall under the definition of an EHR system.[61] In the EHDS proposal, an EHR systems is defined as 'any appliance or software intended by the manufacturer to be used for storing, intermediating, importing, exporting, converting, editing or viewing electronic health records'.[62] The first part of the definition mentions 'any appliance and software'. This definitioncould be met, as medical devices may comprise software.[63] The second part of the definition requires that the software in question shall process EHR. EHR comprises a collection of electronic health data that are related to a natural person and are collected, according to Article 2(2)(m) of the proposal, 'in the health systems' and that shall be processed for healthcare purposes.[64] In principle, it is possible that medical device software can store or import EHR retrieved from the healthcare system. Let us think, for example, of certain elements of a patient's summary, such as their personal details, medical history or plan of care; the software may be used in eHealth settings to draw on a patient's records to provide them with health-related recommendations (e.g., to set reminders or take prescriptions).[65] In light of this, we conclude – as some healthcare stakeholders also suggest[66] – that the current version of the proposal allows us to consider that some medical devices may qualify as EHR systems.[67]

[61] Under the EHDS proposal, an EHR system refers to "any appliance or software intended by the manufacturer to be used for storing, intermediating, importing, exporting, converting, editing or viewing electronic health records" (art. 2(2)(n), EHDS proposal). Its relevance to medical devices will be explained further in section 4.
[62] EHDS proposal, supra note 7, art. 2(2)(n).
[63] See the MDR definition of medical device in art. 2(1), which states "'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." (Emphasis added).
[64] EHDS proposal, supra note 7; art. 2(2)(m) states: "'EHR' (electronic health record) means a collection of electronic health data related to a natural person and collected in the health system, processed for healthcare purposes."
[65] For a list of elements that may be contained by a patient's summary, see the EHDS proposal, supra note 7, Annex I. These include personal details, contact information, allergies, medical alerts, textual information related to medical history, patient provided data, and plan of care.
[66] See COCIR, "COCIR Feedback."
[67] For similar questions in other legal systems outside the EU, see Konnoth, "Are Electronic Health Records Medical Devices?"

What then of the cybersecurity requirements contained in the EHDS proposal and their consequences for medical devices (that are considered EHR systems)? The subsumption of medical devices within the category of EHR systems entails the possibility that manufacturers of medical devices will have to consider the essential requirements laid down in the EHDS proposal; that is, the security requirements for EHR systems.[68] These security requirements for EHR systems are contained in Annex II of the EHDS proposal, under Section Three, titled 'Requirements for security'. They include design and development rules to ensure the safe and secure processing of electronic health data and the prevention of unauthorised access to such data.[69] In addition, the EHR systems designed to be used by health professionals are required to provide reliable mechanisms for the identification and authentication of health professionals, including checks on professional rights and qualifications.[70] Further rules require logging mechanisms, access restrictions, support of digital signatures, consideration of different retention periods and access rights, and identification mechanisms.[71] As a general rule, the manufacturers of EHR systems must comply with these essential requirements with the common specifications that the European Commission may issue in the future.[72] Once manufacturers demonstrate compliance with the essential requirements, they can affix the Conformité Européenne (CE)-marking and place the systems on the market.[73]

In relation to the question of whether (or when) a medical device qualifies as an EHR system, some stakeholders (with whom we agree) are of the opinion that the text of the EHDS proposal is unclear when it comes to this issue.[74] It would be much more desirable that the text explains with greater detail if and when medical devices constitute EHR systems. In relation to the cybersecurity requirements, there are also unanswered questions about the application (and interplay) of the EHDS proposal with the EU MDR. Article 14, titled the 'Interplay with legislation governing medical devices and AI systems', reads: 'EHR systems intended by their manufacturer for the primary use of priority categories of electronic health data referred to in Article 5 shall be subject to the provisions laid down in this Chapter' (which is the chapter that sets out the main requirements for EHR systems).[75] The wording in Article 14, 'intended by the manufacturer', could be problematic.[76] In fact, as it is formulated, this provision could delegate the application of the proposed regulation to the *manufacturer's intention*.[77] Consider, for example, a medical device that processes the priority categories of data but is not *explicitly* intended by the manufacturer to be used to process them. In such a case, the device will not likely qualify as an EHR system, as the manufacturer did not declare it.[78] Consequently, if the manufacturer does not declare that the device is manufactured with the specific intention to, for instance, access patients' health records, then there is no implication that the EHDS proposed regulation applies. Ultimately, that would mean that the safety requirements, including those on the security of EHR systems, are not to be applied even if, *in concreto*, the device processes health records, and health data constitute priority categories of health data. Since the types of data included in the priority categories of electronic health data (and especially patient summaries) are quite broad, manufacturers could have a margin to manoeuvre in determining their intention.[79]

[68] COCIR and other stakeholders criticise the definition of EHR systems as very broad and note that it will "potentially encompass all medical devices which store, intermediate, import, export, convert, edit or view electronic health records and thus make the delineation between EHR systems, medical devices and high-risk AI systems very challenging" (see COCIR, "COCIR Feedback," 3). As they point out, interpretative problems will concern not only medical devices and EHR systems in the EHDS but also medical devices and high-risk AI systems in the proposed AI Act.
[69] EHDS proposal, supra note 7, Annex II, Req. 3.1.
[70] EHDS proposal, supra note 7, Annex II, Req. 3.2.
[71] EHDS proposal, supra note 7, Annex II, Req. 3.3–3.9.
[72] EHDS proposal, supra note 7, art. 17(a).
[73] EHDS proposal, supra note 7, arts. 26, 27.
[74] MedTech Europe, "MedTech Europe's Position."
[75] The EHDS proposal establishes a set of priority categories of personal electronic health data for primary use (EHDS proposal, supra note 7, art. 5). Priority categories of electronic health data include patient health summaries, electronic prescriptions, electronic dispensations, medical images and image reports, laboratory results, and discharge reports. Annex I of the proposal further exemplifies these categories.
[76] This formulation is also present in the definition itself of EHR system (as "any appliance or software intended by the manufacturer …," EHDS proposal, supra note 7, art. 2(2)(n)).
[77] The concept of the intention of the medical device manufacturer has been seen as being problematic in other respects. See Ludvigsen, "When Is Software a Medical Device?"
[78] Emphasis added. The wording is used specifically in the recitals (EHDS proposal, supra note 7, rec. 28).
[79] Finally, as an additional note concerning the interplay of the EHDS with other laws, some EHR systems' security requirements (see above) may overlap with the existing requirements in the MDR and GDPR. When the EHDS Regulation is approved, the existing guidance on medical device cybersecurity will have to be updated and offer new insights about the intersections of medical devices with AI and Data Laws. MDCG, "MDCG 2019-16."

Next, let us examine the security requirements for health data sharing. First, we demonstrate how the EHDS proposal sets requirements for the cybersecurity of health data sharing. Second, we discuss the said requirements by highlighting their possible shortcomings.

4.2 Cybersecurity of Health Data Sharing

In the EHDS proposal, the rules on cybersecurity health data sharing are present under the requirements for the 'secure processing environment' for the secondary use of health data. As indicated in section two, 'secure processing environments' were established by the Data Governance Act and defined as 'the physical or virtual environment and organisational means (…) to allow the entity providing the secure processing environment to determine and supervise all data processing actions, including the display, storage, download and export of data and the calculation of derivative data through computational algorithms'.[80] The EHDS proposal refers to the Data Governance Act and defines it the environment in which the secondary use of electronic health data is deemed to take place.

According to the EHDS proposal, the secure processing environment is expected to be run by health data access bodies that are supposed to facilitate data sharing and that will have to be appointed or established by every Member State once the Regulation is approved.[81] There are conditions and specific purposes for which electronic health data can be shared in those environments.[82] Among the purposes for the secondary use of electronic health data, the proposed regulation includes the 'training, testing and evaluating of algorithms, including in medical devices (…)',[83] scientific research and the provision of personalised healthcare. Thus, these regulations are relevant to medical devices.[84] Data access bodies are required to provide access to electronic health data only in a secure processing environment, and Article 50 of the proposal provides examples of the security measures required in this respect. These include data access management provisions and the risks of reading, copying, modifying or removing electronic health data or log accesses.[85]

The provisions that concern health data sharing in the EHDS proposed regulation may give rise to some uncertainties. We focus on the main issue (i.e., anonymisation in health data sharing and re-identification risks for patients). According to certain stakeholders, despite the focus on the 'security' of the processing environment, the proposal does not set higher standards.[86] The European Digital Rights organisation has recently highlighted that such a space would enhance the risks of re-identification of patients.[87]

We provide an example of how this issue could be problematic in practice: A patient's health data processed by medical device software are further used to provide personalised healthcare services.[88] These data are put in a secure processing environment to allow their further processing. The data holder (the medical device manufacturer or the healthcare provider)[89] anonymises the patient's data before entering the secure processing environment, but the data access bodies conduct no risk assessment for re-identification risks within the same environment. Some malicious actors access the secure processing environment and re-identify the individual's health data. Malicious actors could then use this patient's data to manipulate them (e.g., take advantage of their anxiety or depression) or exploit their data economically (e.g., by illegally selling the data to data brokers).

[80] Data Governance Act, supra note 10, art. 2(20).
[81] As per the EHDS proposal's Explanatory Memorandum, setting up these entities should help ensure a "predictable and simplified access to electronic health data and a higher level of transparency, accountability and security in data processing." EHDS proposal, supra note 7, Explanatory Memorandum, 15.
[82] Conditions and purposes are listed under Chapter IV of the EHDS proposal, titled "Secondary use of electronic health data" (see especially, art. 34 on the purposes for which electronic health data can be processed for secondary use, and art. 35 on the prohibited secondary use of electronic health data).
[83] EHDS proposal, supra note 7, art. 34(1)(g).
[84] EHDS proposal, supra note 7, art. 34.
[85] EHDS proposal, supra note 7, art. 50.
[86] See European Digital Rights, "EHDS: Ignoring Patients' Privacy."
[87] European Digital Rights, "EHDS: Ignoring Patients' Privacy."
[88] The example is taken from one of the purposes for which electronic health data can be processed for secondary use. See EHDS proposal, supra note 7, art. 34(1)(h): "providing personalised healthcare consisting in assessing, maintaining or restoring the state of health of natural persons, based on the health data of other natural persons".
[89] In the EHDS, a data holder is defined as "any natural or legal person, which is an entity or a body in the health or care sector, or performing research in relation to these sectors, as well as Union institutions, bodies, offices and agencies who has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation implementing Union law, or in the case of non-personal data, through control of the technical design of a product and related services, the ability to make available, including to register, provide, restrict access or exchange certain data" (EHDS proposal, supra note 7, art. 2(2)(y). Data "holdership" may require broader considerations. For reasons of space, this article cannot detail them.

Part of the above security concern is addressed by Article 44 of the proposal, which sets out the rules on data minimisation and purpose limitation. The Article specifies that health data bodies shall provide the electronic health data in an anonymised format, and if the purpose of the processing cannot be achieved with such data, then the health data access bodies shall provide access to electronic health data in a pseudonymised format. When submitting a data access application to the health data access body for health data in a pseudonymised format, applicants should provide additional information, consisting of a description of how the processing would comply with the GDPR's legal bases for the processing of personal data and information on the assessment of ethical aspects of the processing, where applicable and in line with national law.[90] Further, Article 44(3) of the proposal prohibits data users from re-identifying the electronic health data provided in a pseudonymised format.

These provisions go some way to dispelling concerns; however, they may not go far enough. For instance, some have argued that anonymisation and pseudonymisation are not sufficient in terms of security measures.[91] Significantly, it seems like this concern has been substantiated by developments regarding the interpretation of 'anonymisation' and 'pseudonymisation' by the European Court of Justice.[92] The recent case of *Single Resolution Board v European Data Protection Supervisor* seemingly allows for an expansive interpretation of 'anonymised data'. There, the European Court of Justice overrode the EU's traditional stance on the matter.[93] The traditional view required that the risk of re-identification should be assessed against any potential entity. Conversely, the ruling maintained that identifiability has to be assessed by considering the potential means that *only the third data sharing party* could use. In practical terms, the ruling is less restrictive in its interpretation of anonymisation. Given this, it is likely that data-sharing stakeholders will consider data anonymous despite their concrete risks of identifiability.[94] Therefore, as a further security measure, the legislature should consider expanding the safeguards for anonymised data provided in Article 45(4) to also cover pseudonymised data. Enhancing these requirements could ultimately benefit patients, as a lack of security standards could affect their autonomy and undermine their trust in the data-sharing system.

Finally, the issue of re-identification risks may also reflect the broader issue of risk-management activities to be carried out by the data access bodies. As the data access bodies will likely be storing and processing large amounts of highly sensitive data, it may be appropriate to consider establishing higher cybersecurity requirements for them. If a cyber-attack targets a data access body, there could be a disruption of services impacting public safety, security and health. Article 50(5) specifies that by implementing regulations, the Commission shall provide for the technical, information security and interoperability requirements of the secure processing environment.[95] However, more attention should be paid to whether *data access bodies* should follow cybersecurity risk-management requirements or even whether they should have notification duties in case of a cyber-attack or threat. Future research should further examine whether it would be appropriate to consider data access bodies within the scope of the NIS2 Directive.[96]

4.3 The Data Act at the Intersection with Cybersecurity Laws

As explained earlier, the Data Act proposal is deemed to apply to medical devices. For example, for business-to-consumer data sharing, the Recitals of the proposal mention medical devices as physical products that might be within the scope of future regulation (Recital 14).[97] The cybersecurity-related provisions of the Data Act of relevance to our discussion are contained in the business-to-government data sharing rules of the proposed regulation. Specifically, they are contained in Chapter V of the Data Act proposal, titled 'Making data available to public sector bodies, the Commission, the European Central Bank or Union bodies based on exceptional need', which are also referred to as 'business-to-government data sharing'.[98] What we are about

[90] EHDS proposal, supra note 7, art. 45(4).
[91] See European Digital Rights, "Make European Health Data Space." Rec. 43 of the EHDS proposal recommends that health data access bodies to "apply techniques that ensure electronic health data is processed in a manner that preserves the privacy of the information contained in the data for which secondary use is allowed (…)." However, its insertion in the recitals does not render it a mandatory requirement for the data access bodies, as the recitals of EU text are not legally binding in nature.
[92] European Court of Justice, Judgement of 26 April 2023, *Single Resolution Board (SRB) v European Data Protection Supervisor (EDPS)*, T-557/20, ECLI:EU:T:2023:219.
[93] Article 29 Working Party, Opinion 05/2014.
[94] In essence, the decision shifts the boundaries of the notion of anonymised data. For a more detailed explanation see Curreli, "Pseudonymization and Anonymization."
[95] Implementing regulations or acts are specific types of laws of the European Union. The European Commission (or in exceptional cases the Council of the European Union) may be given the powers to adopt implementing acts by the EU legislature — through specific rules included in a legislative act (the "basic act") – in this case, the future EHDS regulation.
[96] NIS2 Directive, supra note 4.
[97] See Data Act proposal, supra note 10, rec. 14: "Physical products that obtain, generate or collect, by means of their components, data concerning their performance, use or environment and that are able to communicate that data via a publicly available electronic communications service (often referred to as the Internet of Things) should be covered by this Regulation. (…) Such products may include vehicles, home equipment and consumer goods, medical and health devices or agricultural and industrial machinery."
[98] For a broader analysis on the Data Act proposal, see Ducuing, "White Paper Data Act Proposal."

to see, however, is that the provisions dedicated to cybersecurity in the Data Act proposal are vague, and that vagueness may entail legal uncertainty.

Article 14 of the Data Act proposal establishes the obligation to make available data to public sector bodies, the Commission, the European Central Bank or Union bodies, while Article 15 explains the conditions for the exceptional need to use data. An exceptional need to use data may exist, *among other things*, where the data requested is necessary to respond to a public emergency, or where the data is necessary to prevent or assist the recovery from it. These provisions are relevant from a cybersecurity perspective. Recital 57 of the initial Commission's proposal on the Data Act suggested that human-induced major disasters and *major cybersecurity incidents* should be considered public emergencies. Consider the following example:

A national network of healthcare providers suffers a cyber-attack by exploiting an unknown vulnerability of a medical device with a subsequent data leakage of several patients' health data. Healthcare providers face services and data unavailability, causing problems in their activities, such as enrolling patients in emergencies or treating patients with severe conditions. A public sector body might ask the medical device manufacturer or the healthcare facility to share data with them to study how to prevent such an exceptional threat in the future. The user of the technology is concerned about the consultation of their data by the government and asks about the specific conditions that made the data sharing possible.

The initial version of the Data Act proposal referred to cybersecurity only in its Recitals. In EU law, however, the mention as a recital only implies the non-binding nature of the reference. The latest version of the Data Act proposal not only conserved the reference to cybersecurity but added further substantiation dedicated to definitions.[99] Thus, Article 2(10) of the Data Act proposal (Council version) now contains the explicit definition of 'public emergency' by also including major cybersecurity incidents. The Article states that 'public emergency means an exceptional situation such as public health emergencies, emergencies resulting from natural disasters, as well as human-induced major disasters, *such as major cybersecurity incidents* (…)'. (emphasis added).[100] The article follows and clarifies that an exceptional situation is one that is negatively affecting the population of the Union, a Member State 'with a risk of serious and lasting repercussions on living conditions or economic stability, or the substantial degradation of economic assets' within the EU or the Member States.[101] Finally, the definition requires that the existence or likely occurrence of it is 'determined or officially declared according to the respective procedures under Union or national law'.[102]

The main challenge with these provisions is that the key working concept on which the requirement turns (i.e., 'major cybersecurity incidents') is exceedingly vague. The initial proposal offered no threshold nor specifics to help qualify the range of 'major cybersecurity incidents'. One would have expected further alignment or a reference with existing Cybersecurity Laws, such as the NIS2 Directive or the Cybersecurity Act (as they concern cybersecurity incidents or, as seen above, they contain the definition of 'cybersecurity'). It is worth noting that from the initial version, the Council version added a minor change to the notion of public emergency by requiring its determination by Union or national law. Despite this addition, the new version does not add substantial elements for the specific case of cybersecurity. Further, this vagueness may have some implications. For example, patients' trust in the broader healthcare system could be undermined if they know that public sector bodies could ask for access to their data in case of a 'major cybersecurity incident' whose prerequisites are unclear or undefined. They might even be discouraged from taking advantage of health technologies' functionalities for fear of unduly sharing their data in those situations.

This issue arises from the EU legislature's approach, which in essence creates a misalignment with the existing Cybersecurity Laws. This misalignment could be remedied by aligning these new regulations with the existing cybersecurity concepts instead of creating new ones (as we noted above). In conclusion, as it stands, the proposal is in an urgent need of clarification. In the final stages of its making, the legislature should consider whether it is appropriate to include major cybersecurity incidents within the scope of the Data Act. If they decide that this is appropriate, the definition should offer concrete criteria for its application in those circumstances.

[99] Data Act proposal, Council version.
[100] Data Act proposal, supra note 99, art. 2(10).
[101] Data Act proposal, supra note 99.
[102] Data Act proposal, supra note 99.

Conclusion

This article discussed the potential shortcomings that the EU legislature's approach could result in after the adoption of the new proposed regulations, such as the new Data and AI Laws, in the context of the medical device cybersecurity legal framework. First, we observed that the medical device cybersecurity legal framework is composed, as illustrated in section two, of an array of different kinds of laws. These include Medical Device Law (including the EU MDR and IVDR), Cybersecurity Laws (including the Network Information System Directives and the Cybersecurity Act), AI Laws (including the proposed AI Act) and Data Law (including the GDPR, the Data Governance Act, the forthcoming EHDS Regulation and Data Act).

To illustrate the shortcomings of the EU approach, we identified the specific challenges arising in different laws for medical device cybersecurity. Notably, we commented on the new cybersecurity requirements comprised in AI Laws and more specifically, by the AI Act. We discussed the fact that the AI Act could (also) be considered a cybersecurity regulation and commented on how it raises two main issues. Notably, we observed that the AI Act does not refer explicitly to the Cybersecurity Act's definition of cybersecurity – a particularly important aspect that would establish a stronger link to an individual's cybersecurity protection. Second, we highlighted that the AI Act proposal mentions only technical measures and falls short in considering organisational measures to ensure the cybersecurity of high-risk AI systems, which are required by Cybersecurity Laws. These two issues can be seen as a symptom of a lack of full alignment with existing Cybersecurity Laws.

Following this, in section four, we examined the new cybersecurity rules comprised in the forthcoming Data Laws. We first analysed the EHDS proposal, pointing out the intrinsic problems of the proposed regulation (i.e., that it is unclear whether medical devices could be considered EHR systems, but if they are, we argued that the delegation of their qualification to the *intention* of the manufacturers could be problematic). Then, we commented on the insufficient cybersecurity requirements of the secure processing environment (which could thus expose patients to re-identification risks and privacy breaches) and the missed opportunity to consider health data access bodies within the ambit of the NIS2 Directive. The second part of section four commented on the Data Act rules on business-to-government data sharing and its notion of 'major cybersecurity incidents'.

We underlined that these provisions may cause legal uncertainty and is not fully aligned with definitions in Cybersecurity Laws. Our analysis of the general approach of the EU showed that new Data Laws and AI Laws will introduce new cybersecurity requirements that add to the existing Cybersecurity Laws. However, these are either insufficient as cybersecurity measures or do not fully align with the existing Cybersecurity Laws. For example, the AI Act proposal does not fully align with the Cybersecurity Act; the Data Act proposal does not consider the existing Cybersecurity Laws in their definition of 'major cybersecurity incident'; and the EHDS proposal establishes entities for monitoring secure processing environments but does not consider their relevance from a cybersecurity point of view.

In light of these challenges, the following recommendations to the EU legislature can be made in relation to the specific regulations covered by this article. First, under the AI Act, it would be desirable that the EU clarifies the definition of cybersecurity in a way that the actual beneficiaries of cybersecurity (e.g., patients and individuals) can be protected. Second, with regard to the EHDS proposal, legislators should consider enhancing security measures for the secure processing environments of EHRs. This could be done by expanding the requirements of Article 45(4) of the EHDS proposed regulation to also cover anonymised data. In addition, EU lawmakers should consider clarifying whether medical devices could be considered EHR systems and whether data access bodies should be included within the scope of the NIS2 Directive. Third, the Data Act proposal could be enhanced by making the notion of 'major cybersecurity incidents' clearer or linked to other Cybersecurity Laws. These actions would ultimately enhance legal certainty, ensure higher privacy and security standards and foster individuals' and patients' trust in the healthcare system.

Finally, given the broader issues we identified in this article, we suggest that before issuing any new laws with cybersecurity requirements, EU legislators assess any possible links to existing Cybersecurity Laws. Such an assessment could avoid possible inconsistencies or overlaps in different pieces of legislation and ensure their best alignment with Cybersecurity Laws.

Bibliography

Article 29 Working Party. *Opinion 05/2014 on Anonymisation Techniques,* 2014.

Biasin, Elisabetta and Erik Kamenjašević. "Cybersecurity of Medical Devices: Regulatory Challenges in the European Union." In *The Future of Medical Device Regulation: Innovation and Protection*, edited by I Glenn Cohen, Timo Minssen, W Nicholson Price Ii, Christopher Robertson and Carmel Shachar, 1st ed., 51–62. Cambridge: Cambridge University Press. https://doi.org/10.1017/9781108975452.005.

Biasin, Elisabetta and Erik Kamenjašević. "Cybersecurity of Medical Devices: New Challenges Arising from the AI Act and NIS 2 Directive Proposals." *International Cybersecurity Law Review* (2022): 163–180. https://doi.org/10.1365/s43439-022-00054-x.

Bygrave, Lee A. "Security by Design: Aspirations and Realities in a Regulatory Context." *Oslo Law Review* 8, no 3 (June 7, 2022): 126–77. https://doi.org/10.18261/olr.8.3.2.

Chiara, Piergiorgio. "The IoT and the New EU Cybersecurity Regulatory Landscape." *International Review of Law, Computers and Technology*, 36, no 2 (May 4, 2022). https://doi.org/10.1080/13600869.2022.2060468.

Curreli, Eleonora, Laura Liguori and Elena Mandarà. "Pseudonymization and Anonymization of Data: Recent Developments from European Case-Law." Portolano Cavallo, May 31, 2023. https://portolano.it/en/newsletter/portolano-cavallo-inform-digital-ip/pseudonymization-anonymization-data-recent-developments-from-european-case-law.

Directive (EU) 2016/1148 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.

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).

Ducuing, Charlotte; Thomas Margoni, Luca Schirru, Daniela Spajic, Teodora Lalova-Spinks, Leander Stähler, Emre Bayamlıoğlu, Antoine Pétel, Jungyi Chu, Bert Peeters, Athena Christofi, Julie Baloup, Maria Avramidou, Aliki Benmayor, Thoma Gils, Eyup Kun, Eyup; Ella De Noyette, Elisabetta Biasin. "White Paper on the Data Act Proposal." *SSRN Electronic Journal*, 2022. http://dx.doi.org/10.2139/ssrn.4259428.

European Commission. "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.

European Commission. "Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space," COM(2022) 197 final.

European Commission. "Proposal for a Regulation of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data (Data Act)," COM(2022) 68 final.

European Commission. "Proposal for a Regulation of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data (Data Act) – Mandate for Negotiations with the European Parliament," 2022/0047(COD)

European Commission. *Report on the Safety and Liability Implications of Artificial Intelligence, the Internet of Things and Robotics* (European Commission, 2020)*., 19 February 2020, COM (2020) 64 final*.

European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry (COCIR). "COCIR Feedback – Proposal for a European Health Data Space." July 27, 2022. https://www.medtecheurope.org/wp-content/uploads/2023/02/230222-ehds-position-paper-final.pdf.

European Court of Justice, Judgement of 26 April 2023, *Single Resolution Board (SRB) v European Data Protection Supervisor (EDPS)*, Case T-557/20, ECLI:EU:T:2023:219.

European Digital Rights, "Make the European Health Data Space Serve Patients and Research," European Digital Rights, 2023, https://edri.org/wp-content/uploads/2023/03/EHDS-EDRi-position-final.pdf.

European Digital Rights. "EHDS: Ignoring Patients' Privacy." European Digital Rights (EDRi), March 6, 2023. https://edri.org/our-work/eu-proposed-health-data-regulation-ignores-patients-privacy-rights/.

European Parliament, *Draft Compromise Amendments on the Draft Report* (European Parliament, 16 May 2023).

Fuster, Gloria González and Lina Jasmontaite. "Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights." In *The Ethics of Cybersecurity*, edited by Markus Christen, Bert Gordijn and Michele Loi, 97–115. Cham: Springer International Publishing, 2020.

Jasmontaite, Lina, Irene Kamara, Gabriela Zanfir-Fortuna and Stefano Leucci. "Data Protection by Design and by Default:" *European Data Protection Law Review* 4, no 2 (2018): 168–89. https://doi.org/10.21552/edpl/2018/2/7.

Konnoth, Craig. "Are Electronic Health Records Medical Devices?" In *The Future of Medical Device Regulation*, edited by I. Glenn Cohen, Timo Minssen, W. Nicholson Price Ii, Christopher Robertson and Carmel Shachar, 1st ed., 36–46. Cambridge University Press, 2022. https://doi.org/10.1017/9781108975452.004.

Ludvigsen, Kaspar Rosager, 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 EU Law." *European Journal of Risk Regulation* 13, no 1 (2022). 78-93. https://doi.org/10.1017/err.2021.45.

Ludvigsen, Kaspar Rosager. The Role of Cybersecurity in Medical Devices Regulation: Future Considerations and Solutions, *Law, Technology and Humans* 5, no 2, (2023): 59-77. https://doi.org/10.5204/lthj.3080.

Medical Device Coordination Group. *MDCG 2019-16 Guidance on Cybersecurity for Medical Devices* (Medical Device Coordination Group, 2019).

MedTech Europe. "MedTech Europe's Position on the Proposed European Health Data Space Regulation," February 22, 2023. https://www.medtecheurope.org/news-and-events/news/medtech-europes-position-on-the-proposed-european-health-data-space-regulation/#:~:text=MedTech%20Europe%20believes%20that%20the,European%20market%20for%20digital%20health.

Orlando, Domenico and Pierre Dewitte. "The 'by Design' Turn in EU Cybersecurity Law: Emergence, Challenges and Ways Forward." In *Security and Law*, edited by Anton Vedder, Jessica Schroers, Charlotte Ducuing and Peggy Valcke, 1st ed., 239–52. Intersentia, 2019. https://doi.org/10.1017/9781780688909.010.

Papakonstantinou, Vagelis. "Cybersecurity as Praxis and as a State: The EU Law Path towards Acknowledgement of a New Right to Cybersecurity?" *Computer Law & Security Review* 44 (April 2022): 105653. https://doi.org/10.1016/j.clsr.2022.105653.

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 (GDPR).

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 (Medical Device Regulation or MDR).

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).

Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European Data Governance and Amending Regulation (EU) 2018/1724 (Data Governance Act)

Vedder, Anton. "Safety, Security and Ethics," Vol. 7. Intersentia; Cambridge, Antwerp, Chicago, 2019.

Zanfir-Fortuna, Gabriela. "Tracing the Right to Be Forgotten in the Short History of Data Protection Law: The "New Clothes" of an Old Right" in *Reforming European Data Protection Law*, edited by Serge Gutwirth, Ronald Leenes and Paul de Hert, Law, Governance and Technology Series, Springer, 2015.