4

Cybersecurity of Medical Devices

Regulatory Challenges in the European Union

Elisabetta Biasin and Erik Kamenjasevic

4.1 INTRODUCTION

4.1.1 *Context*

Ensuring cybersecurity in the health care sector is a growing concern. The increasing digitalization of health care service providers has enabled cyberattack techniques toward them to become more liquid, flexible, and able to exploit all the possible paths of entry rapidly.[1] For example, one such attack may target critical assets of hospitals which include both the IT infrastructure and connected-to-network medical devices. A successful cyberattack toward IT infrastructure may cause significant disruptive effects for the provision of essential health care services.[2] When a cyberattack concerns a medical device, it may put at severe risk the health and safety of patients.[3] This disquiet appears to be even greater at the time of a worldwide COVID-19 outbreak. Reports on cyberattacks toward medical devices issued during this pandemic revealed how hackers use various techniques to get access to individuals' sensitive health-related information for different gains.[4]

The authors wish to thank: Prof. W. Nicholson Price II, Charlotte Ducuing, and Jessica Schroers for their helpful comments and feedback. The research leading to these results has received funding from the European Union's Horizon2020 Research and Innovation Programme, under Grant Agreement no 787002.

1 Enrico Frumento, Cybersecurity and the Evolutions of Healthcare: Challenges and Threats Behind its Evolution, in m_Health Current and Future Applications 115 (Giuseppe Andreoni et al. eds., 2019).

2 This happened, for instance, during the Wannacry malware attacks for several trustees of the UK National Healthcare System (NHS). See Finnian Bamber et al., Nat'l Audit Office, Investigation: Wannacry Cyber-Attack and the NHS (2018).

3 As was demonstrated in 2018 by a team of researchers, an attacker could cause pacemakers to deliver a deadly shock or stop an insulin pump from providing the needed insulin to a patient. See Sally Shin & Josh Lipton, Security Researchers Say They Can Hack Medtronic Pacemakers, CNBC (Aug. 17, 2018), www.cnbc.com/2018/08/17/security-researchers-say-they-can-hack-medtronic-pacemakers.html.

4 See Laurens Cerulus, Hackers Use Fake WHO Emails to Exploit Coronavirus Fears, POLITICO (Mar. 13, 2020), www.politico.eu/article/hackers-use-fake-who-emails-to-exploit-coronavirus-fears-for-gain/?fbclid=IwAR379JroScZEggppneFxEQqMpYfKP9M0Rg90k1lB-xziGkIH_3Byy1NtKjE; Mathew M. Schwartz, COVID-19 Complication: Ransomware Keeps Hitting Healthcare, Bank Info Security

https://doi.org/10.1017/9781108975452.005 Published online by Cambridge University Press

Regulators around the globe have started increasingly to pursue medical device cybersecurity as a policy objective over the past years. For example, the US Food and Drug Administration (FDA) issued its first general principles for Networked Medical Devices Containing Off-the-Shelf Software in 2005, followed by the 2014 and 2016 Guidance for Premarket Submission and Postmarket Management of Cybersecurity in Medical Devices. In March 2020, the International Medical Devices Regulators Forum (IMRDF) issued its medical devices principles and practices on medical devices' cybersecurity, while in the European Union (EU), the first piece of guidance was issued only in July 2020 (with the first version from December 2019) by the European Commission's (EC) Medical Devices Coordination Group (MDCG).

4.1.2 *Ambition*

Discussions evolving around the regulation of medical devices and their cybersecurity are a recent trend in academic literature.[5] Many contributions analyze the US system, while fewer concern the EU one.[6] This chapter aims to contribute to the literature dealing with the law of medical devices and cybersecurity by assessing the level of maturity of the EU medical devices legal framework and EU cybersecurity policy objectives.[7] The analysis starts with an outline of cybersecurity-related aspects of EU Medical Devices Regulation (MDR).[8] This is followed by a critical analysis of regulatory challenges stemming from the MDR, through the lens of the MDCG Guidance. The following section concerns the regulatory challenges stemming from other legal frameworks, including the Cybersecurity Act,[9] the Network and Information Systems (NIS) Directive,[10] the General Data Protection Regulation

(Mar. 16, 2020), www.bankinfosecurity.com/covid-19-complication-ransomware-keeps-hitting-hospitals-a-13941.

5 See Deborah Eskenasy, Le dispositif médical à la recherche d'un nouveau cadre juridique 38 (Nov. 30, 2016) (unpublished PhD dissertation) (remarks on legal literature on medical devices law).

6 See, for example, Charlotte A. Tschider, Enhancing Cybersecurity for the Digital Health Marketplace, 26 Ann. Health L. 1 (2017); Louiza Doudin, Networked Medical Devices: Finding a Legislative Solution to Guide Healthcare into the Future, 40 Seattle U. L. Rev. 1085 (2017).

7 Joint Communication to the European parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Cybersecurity strategy of the European union: an open, safe and secure cyberspace, JOIN (2013) 1 final (Feb. 7, 2013) [hereinafter EC 2013 Cybersecurity Strategy].

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

9 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 O.J. (L 151) [hereinafter CSA].

10 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, 2016 O.J. (L 194) [hereinafter NISD].

(GDPR),[11] and the Radio Equipment Directive (RED)[12] since they all become applicable when it comes to ensuring the cybersecurity of medical devices. Here the analysis demonstrates that regulatory challenges persist due to regulatory specialization,[13] which has led to regulatory overlapping, fragmentation risks, regulatory uncertainty, and duplication.[14] In the final section, the chapter provides conclusive remarks as well as recommendations for regulators dealing with the cybersecurity of medical devices in the European Union.

4.2 HOW DOES THE EU MEDICAL DEVICES REGULATION DEAL WITH THE CYBERSECURITY OF MEDICAL DEVICES?

The provisions of the EU Medical Devices Regulation (MDR)[15] primarily address manufacturers of medical devices who are defined as "the natural or legal person who manufactures or fully refurbishes a device or has a device designed, manufactured, or fully refurbished and markets that device under its name or trademark."[16] No explicit reference to cybersecurity is provided in the main part of the MDR. However, it provides some essential cybersecurity-related requirements that manufacturers have to implement in a medical device.[17]

When putting a medical device on the market or into service, Article 5(1) of the MDR obliges its manufacturer to ensure that the device is compliant with the MDR obligations when used in accordance with its intended purpose. According to Article 5(2) of the MDR, "a medical device shall meet the general safety and performance requirements" (also including the cybersecurity-related requirements)[18] "set out in Annex I [of the MDR] ... taking into account the

[11] 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 O.J. (L 119) [hereinafter GDPR].

[12] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonization of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC, 2014 O.J. (L 153) [hereinafter RED].

[13] See Emmanuelle Mathieu et al., 2011, Regulatory Agencies and Multi-Actor Regulatory Governance: A Method to Study Regulatory Fragmentation, Specialization, Coordination and Centralization (unpublished manuscript) (2011), www.academia.edu/20494619/Regulatory_agencies_and_multi-actor_regulatory_governance_A_method_to_study_regulatory_fragmentation_specialization_coordination_and_centralization (on the notion of specialization and fragmentation).

[14] In this chapter, we will refer to "cybersecurity" in two different ways. In a general way, we mean "cybersecurity" as a policy objective pursued by the European Union – having regard to the EC 2013 Cybersecurity Strategy (see supra note 7). When used in a specific way, we refer to the definition provided by the CSA, art. 4: "a set of activities to protect network and information systems the users of such systems, and other persons affected by cyber threats."

[15] MDR, supra note 8.

[16] Id. art. 2(30).

[17] See Medical Devices Coordination Group, Guidance on Cybersecurity of medical devices (Dec. 2019) [MDCG, Guidance] (complete list of the cybersecurity requirements).

[18] Id.

https://doi.org/10.1017/9781108975452.005 Published online by Cambridge University Press

intended purpose."[19] The intended purpose is defined in Article 2(12) as "the use for which a device is intended according to the data supplied by the manufacturer on the label, in the instructions for use or in promotional or sales materials or statements and as specified by the manufacturer in the clinical evaluation." As part of the general requirements set in Annex I of the MDR, "devices shall achieve the performance intended by the manufacturer"[20] and be designed in a way suitable for the intended use. They shall be safe and effective, and associated risks shall be acceptable when weighed against the benefits of the patients and level of protection of health and safety while taking into account the state of the art.[21]

Moreover, "[m]anufacturers shall establish, implement, document, and maintain a risk management system."[22] Part of this system also includes risk-control measures to be adopted by manufacturers for the design and manufacture of a device, and they shall conform to safety principles and state of the art.[23] A medical device designed to be used with other devices/equipment as a whole (including the connection system between them) has to be safe and should not impair the specified performance of the device.[24]

Furthermore, a medical device shall be designed and manufactured in a way to remove, as far as possible, risks associated with possible negative interaction between software and the IT environment within which they operate.[25] If a medical device is intended to be used with another device, it shall be designed so the interoperability and compatibility are reliable and safe.[26] A medical device incorporating electronic programmable systems, including software or standalone software as a medical device, "shall be designed to ensure repeatability, reliability, and performance according to the intended use,"[27] and "appropriate means have to be adopted to reduce risks or impairment of the performance."[28] A medical device should be developed and manufactured according to the state of the art and by respecting the principles of the development lifecycle, risk management (including information security), verification, and validation.[29] Lastly, manufacturers shall "set out minimum requirements concerning hardware, IT network characteristics, and IT security measures, including protection against unauthorized access."[30] Concerning information to be supplied together with the device,

[19] MDR, supra note 8, art. 5(2).
[20] Id. Annex I, req. 1.
[21] Id.
[22] Id. req. 3.
[23] Id. req. 4.
[24] Id. req. 14.1.
[25] Id. req. 14.2.(d).
[26] Id. req. 14.5.
[27] Id. req. 17.1.
[28] Id.
[29] Id. req. 17.2.
[30] Id. req. 17.4.

https://doi.org/10.1017/9781108975452.005 Published online by Cambridge University Press

manufacturers must inform about residual risks,[31] provide warnings requiring immediate attention on the label[32] and, for electronic programmable system devices, give information about minimum requirements concerning hardware, IT networks' characteristics, and IT security measures (including protection against unauthorized access), necessary to run the software as intended.[33]

4.3 REGULATORY CHALLENGES STEMMING FROM THE MDR ANALYZED THROUGH THE LENS OF THE MDCG GUIDANCE ON CYBERSECURITY FOR MEDICAL DEVICES

The Medical Device Coordination Group (MDCG) of the European Commission endorsed Guidance on Cybersecurity for Medical Devices (Guidance) in December 2019[34] where it dealt with the cybersecurity-related provisions embedded in the MDR. Already, it is necessary here to mention that this MDCG Guidance is not a legally binding document. Hence, in case of disagreement, manufacturers could decide not to follow it – which might have an impact on the overall harmonizing purpose of the MDR and lead to a divergence of application of the EU principles and laws on a Member State level. Nevertheless, being the first guiding document on this topic issued by the EC for the medical devices sector, it is an essential step in further elaborating on specific MDR cybersecurity-related provisions.

As already mentioned in the previous section, the MDR does not expressly refer to cybersecurity.[35] Nor does the MDCG Guidance define the terms "cybersecurity," "security-by-design," and "security-by-default." Instead, the latter document only provides an outline of its provisions relating to cybersecurity of medical devices and points out conceptual links between safety and security.[36] Leaving these terms theoretical and undefined does not facilitate their implementation in practical terms by the stakeholders concerned.

Moreover, no reference in the MDCG Guidance is given to definitions provided by the Cybersecurity Act (CSA).[37] Establishing a connection in the soft-law instrument (i.e., the Guidance) with the latter would imply a reference to a hard law definition. This link could serve to reduce the ambiguity of the term, and it might help in achieving more coherence within the EU cybersecurity regulatory framework as a whole.[38] The

[31] Id. req. 23.1.(g).
[32] Id. req. 23.2.(m).
[33] Id. req. 23.4.(ab).
[34] MDCG, Guidance, supra note17.
[35] See Elisabetta Biasin, Medical Devices Cybersecurity: A Growing Concern?, CITIP Blog (Sept. 26, 2019), www.law.kuleuven.be/citip/blog/medical-devices-cybersecurity-a-growing-concern/, (a concise overview of cybersecurity, EU guidance and the MDR).
[36] MDCG, Guidance, supra note 17, at 7.
[37] Id. at 9.
[38] See Gloria González Fuster & Lina Jasmontaite, Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights, in The Ethics of Cybersecurity 119 (Markus

https://doi.org/10.1017/9781108975452.005 Published online by Cambridge University Press

proposed approach would be ultimately beneficial for manufacturers as it would bring more clarity in the interpretation of MDR requirements.

The MDCG Guidance stresses the importance to "recognize the roles and expectations of all stakeholders"[39] on joint responsibility and states its "substantial alignment" with International Medical Device Regulators Forum (IMRDF) Principles and Practices for Medical Devices Cybersecurity.[40] To this end, achieving a satisfactory level of the cybersecurity of a medical device concerns manufacturers, suppliers, health care providers, patients, integrators, operators, and regulators. Manufacturers are bound by the majority of the provisions in the MDR. Integrators of a medical device are, among others, responsible for assessing a reasonable level of security while operators need to ensure the required level of security for the operational environment, and that personnel are properly trained on cybersecurity issues. At the same time, health care professionals are responsible for a device being used according to the description of the intended use, while patients and consumers need to "employ cyber-smart behaviour."[41] All of these stakeholders are an equally important part of the cybersecurity chain,[42] and each is responsible for ensuring a secured environment in which a device could smoothly operate for the ultimate benefit of patients' safety.

Nevertheless, the MDCG Guidance failed to elaborate on how exactly the joint responsibility of different stakeholders is influenced or conflicted by other applicable laws, in particular, when it comes to the Network and Information Systems (NIS) Directive,[43] the General Data Protection Regulation (GDPR),[44] and the Cybersecurity Act (CSA).[45] Since the expert group did not tackle them in detail in theory, it is also hard to imagine how the interested stakeholders operating within the medical devices domain are supposed to implement in practice different pieces of legislation divergent in scope and applicability.[46] Hence, the MDCG should consider adopting a more holistic approach in the future when determining the meaning of "joint responsibility" as this would help in analyzing relevant aspects of other

Christen et al. eds., 2020) (for an overview of the coherence problem in the EU cybersecurity legal framework).

39 MDCG, Guidance, supra note 17, at 12.

40 Id.

41 Id. at 13.

42 See Erik Kamenjasevic, Protect the Weakest Link in a Cyber-Security Chain – Protect the Human, CITIP Blog (Mar. 20, 2018), www.law.kuleuven.be/citip/blog/protect-the-weakest-link-in-a-cyber-security-chain-protect-the-human/.

43 NISD, supra note 10.

44 GDPR, supra note 11.

45 CSA, supra note 9.

46 Further elaboration on these laws could have been done, by the same expert group, based on art. 3(5) and 12 of the Medical Devices Coordination Group Rules of Procedure. art. 3(5) states that the Chair of the MDCG or the working group may invite, on a case-by-case basis, experts and other third parties with specific competence in a subject on the agenda to participate in the meetings or provide written contributions. art. 12 provides that the Commission services shall provide technical, scientific, and logistical support for the MDCG and any of its working groups.

horizontal legislation and, eventually, in achieving a more coherent cybersecurity regulatory framework.

Finally, what seems to be heavily overlooked for unclear reasons is the applicability of the Radio Equipment Directive (RED),[47] which has not even been mentioned in the MDCG Guidance. The RED cybersecurity-related provisions and their interaction with MDR as well as the other laws applicable to the cybersecurity of medical devices are explained below.

4.4 REGULATORY CHALLENGES STEMMING FROM OTHER LEGAL FRAMEWORKS APPLICABLE TO MEDICAL DEVICES

Regulation of cybersecurity is a complex task. Cybersecurity is an area in which different policy fields need to be combined (horizontal consistency), and where measures need to be taken at both levels – the European Union and Member States (vertical consistency).[48] Regulation of medical devices is complex, too, as it is a multi-level[49] legal framework characterized by specialization and fragmentation.[50] Regulating the cybersecurity of medical devices implies bearing the complexities of both legal frameworks. In this regard, we identified four regulatory challenges: regulatory overlapping; fragmentation risks; regulatory uncertainty; and duplication. We clarify the first two challenges as relating to horizontal consistency requirements, the third to vertical requirements, and the fourth to a combination thereof. Finally, we envisage specialization and fragmentation as a common denominator of all four challenges.

4.4.1 *Regulatory Overlapping: CSA Certification Schemes and the MDR*

On the one hand, the MDR provides the possibility to obtain a certificate for demonstrating compliance with its security requirements. On the other hand, the CSA set up a new and broader framework for cybersecurity certifications for ICT products, processes, and services. The CSA appears to be inevitably relevant for medical devices' cybersecurity since medical devices may fall under the definition of an ICT product.[51]

Some stakeholders have questioned the applicability of CSA rules and the operability of European Cybersecurity Certification Schemes (ECCS) for health care.[52] They expressed concerns as regards to overlaps between MDR and cybersecurity

47 RED, supra note 12.

48 Ramses Wessel, Towards EU Cybersecurity Law: Regulating a New Policy Field in Research Handbook on Int'l Law & Cyberspace 405 (Nicholas Tsagourias et al. eds., 2015).

49 See Nupur Choudhoury & Ramses Wessel, Conceptualising Multilevel Regulation in the EU: A Legal Translation of Multilevel Governance?, 18(3) Eur. L.J. 335 (2012).

50 See supra Section 4.1.2.

51 CSA, art. 2(12).

52 See, e.g., COCIR, Advancing Cybersecurity of Health and Digital Technologies (Mar. 27, 2019), www.cocir.org/uploads/media/19036_COC_Cybersecurity_web.pdf.

certification schemes and requirements.[53] For instance, COCIR (the European trade association representing the medical imaging, radiotherapy, health ICT and electromedical industries) claimed that "[a] specific certification scheme for medical devices is … not necessary as the MDR introduces security requirements that will become part of the certification for receiving the CE mark."[54] Such a scenario may bring duplication in requirements for manufacturers on the one hand, as well as for authorities having the oversight on manufacturers' compliance. Ultimately, this could also imply conflicts in authorities' respective competence.

The MDCG Guidance did not provide clarifications on the applicability of the CSA in this context. It provides only one reference to the CSA in the whole body of the document.[55] The reference is purely descriptive[56] and does not resolve the applicability question. Against this background, the CSA clarifies that the health care sector should be one of its priorities.[57] The MDCG or the EU regulator should provide further guidance tackling aspects relevant to the cybersecurity certification schemes for medical devices. This could be done, for instance, by explaining how MDR cybersecurity-related requirements apply when the ICT product is considered to be a medical device and what type of certification schemes would be relevant. Furthermore, regulators could specify that, for ICT products not qualifying as a medical device, the CSA should remain the general rule.

4.4.2 *Fragmentation Risks: Voluntariety of Certification Mechanisms*

As seen in Section 4.4.1, the CSA has established certification mechanisms for ensuring the cybersecurity of ICT products. Manufacturers of medical devices may join them voluntarily.[58] However, EU Member States may establish a mandatory certification mechanism in their territories since the CSA provides that "[t]he cybersecurity certification shall be voluntary *unless otherwise specified by Union law or Member State law*" (emphasis added).[59] In practice, this provision implies that some Member States may impose the obligation of obtaining a cybersecurity certification, while others would leave it as a voluntary fulfilment. Manufacturers would be obliged to obtain a cybersecurity certificate for a device to market it within one Member State while at the same time, the same would not be required in another Member State.

[53] See id.
[54] Id. at 6.
[55] See MDCG, Guidance, supra note 17.
[56] Id.
[57] CSA, art. 56(3).
[58] CSA, art. 56(2).
[59] Id.

https://doi.org/10.1017/9781108975452.005 Published online by Cambridge University Press

This hypothesis could provoke diverging mechanisms in the internal market and could lead to regulatory shopping.[60] Manufacturers could also face additional compliance costs for aligning with different national requirements. Moreover, this could lead to fragmentation risks for the EU market. National requirements could diverge, and supervisory authorities could interpret different rules following different interpretative approaches.[61] Therefore, the overarching regulatory strategies to bring more consistency amongst the Member States should aim at ensuring coordination and cooperation amongst competent authorities.

4.4.3 *Regulatory Uncertainty: Security Requirements between the MDR and the Radio Equipment Directive (RED)*

The RED establishes a regulatory framework for making available on the EU market and putting into service of radio equipment. Certain types of medical devices (such as pacemakers or implantable cardioverter defibrillators) are likely to fall under the scope of the Directive and thus be subject to its security requirements.[62] The RED's simultaneous application with the MDR may imply issues in practice. Notably, such parallel application may lead to the question of whether RED security rules are complementary or redundant to the MDR.[63]

The European Commission developed guidance (the RED Guide)[64] to assist in the interpretation of the RED. However, the RED Guide only states that an overlap issue covering the same hazard might be resolved by giving preference to the more specific EU legislation.

Similarly, more general EC guidelines on EU product rules (the Blue Guide)[65] explains first, that two or more EU legislative acts can cover the same product, hazard, or impact. Second, it provides that the issue of overlap might be resolved by

[60] DIGITALEUROPE, Cybersecurity Act: DIGITALEUROPE Urges Colegislators to Ensure Certification Schemes Do Not Lead to More Market Fragmentation in Europe (June 11, 2018), www.digitaleurope.org/wp/wp-content/uploads/2019/01/DIGITALEUROPE%20Cybersecurity%20Act%2011%20June.pdf (stakeholders' concerns over the CSA's fragmentation risks).

[61] See Jan Rommel et al., Specialisation and Fragmentation in Regulatory Regimes, in Government of Public Management 69–71 (Patrick Lægreid et al. eds., 2010).

[62] Amongst the many other aspects, the RED foresees technical features for the protection of privacy, personal data, misuse, interoperability, network functioning, and compliance regarding the combination of radio equipment and software. See RED, art. (3)(3), lett. (d) and (e). Since they relate to network and information systems, the two articles are considered for the purposes of the present chapter as cybersecurity-related requirements.

[63] Due to overlapping elements, manufacturers must refer to different notified bodies to meet obligations stemming from different legislations. In practice this adds another level of complexity. See BSI, Medical Devices complying with the Radio Equipment Directive, www.bsigroup.com/meddev/LocalFiles/ja-jp/Technologies/BSI-md-Radio-devices-ja-JP.pdf.

[64] European Commission, Guide to the Radio Equipment Directive 2014/53/EU, Version of 19 December 2018 (2018) [hereinafter EC, RED Guide].

[65] European Commission, The 'Blue Guide' on the EU Interpretation of EU Product Rules (2014) [hereinafter EC, Blue Guide].

giving preference to the more specific law. This, explains the EC, "usually requires a risk analysis of the product, or sometimes an analysis of the intended purpose of the product, which then determines the applicable legislation."[66] In other words, except for the cases where the applicability of one law has obvious priority over the other, a medical device's manufacturer is left with a choice of the applicable legislation. On the one hand, this approach could imply a significant burden for virtuous manufacturers in justifying the applicable law. On the other hand, such kind of regulatory uncertainty could lead less-virtuous manufacturers to exploit somehow "functional overlaps" of the two regulations and bring them to "choose only" compliance with RED. This could be particularly significant for low-risk medical devices, for which a decision on the intended medical purpose – and thus, law's scrutiny – is left to the responsibility of the manufacturer.[67]

The MDCG Guidance does not provide any help in this regard. For no apparent reasons, it overlooked the applicability of the RED while it should be present in the Guidance. For example, the MDCG could provide an example of cases to which the RED applies, together with its opinion of the relevance of RED cybersecurity-related requirements. This solution would help to resolve regulatory uncertainty and help manufacturers in their decision concerning the applicability of requirements stemming from different pieces of legislation.

4.4.4 *Duplication: The Notification of Medical Devices Security Incidents*

Incident notification is an evident example of how specialization and decentralization have provoked the proliferation of administrative authorities with supervisory tasks. This is particularly true for the framework of medical devices where three different legal frameworks for incident notification apply: the MDR (on serious incident notification),[68] the GDPR (on data breach notification),[69] and the NISD (on security incident notification obligations).[70] Every piece of legislation requires notification to different authorities: the MDR to competent authorities, the GDPR to supervisory authorities, the NISD to national authorities or Computer Security Incident Response Teams (CSIRTs) (depending on the incident reporting model chosen by the Member State).[71] Criteria for which an incident must be notified to an authority differ in scope and objectives pursued by different pieces of legislation.

66 EC, Blue Guide, 22.

67 See Eugenio Mantovani & Pedro Cristobal Bocos, Are mHealth Apps Safe? The Intended Purpose Rule, Its Shortcomings and the Regulatory Options under the EU Medical Devices Framework, in Mobile E-Health 251–76 (Hannah R. Marston et al. eds., 2017) (on pitfalls of the "intended purpose" notion in medical devices law).

68 MDR, art. 87.

69 GDPR, art. 33–4.

70 NISD, art. 14.

71 There are four different incident reporting models: centralized, distributed, decentralized, hybrid. See ENISA, EU MS Response Development Status Report (2019) 8–9.

None the less, it could happen that in practice, a security incident concerning a medical device should be notified at the same time to MDR, NISD and GDPR competent and/or supervisory authorities.[72]

In this case, notification of a security incident implies administrative oversight by three (or more) different authorities. Such a circumstance could cause duplication of tasks and costly compliance procedures for manufacturers and health care stakeholders in general.[73] Some stakeholders already pointed out that "increasing numbers of organizations . . . need to be informed about a single security incident," and "[i]n some examples, multiple competent authorities in a single country."[74]

A possible approach that could simplify the whole process would be to "adopt a more centralized approach to avoid duplication and confusion."[75] A step further could be done by enhancing cooperation mechanisms between these authorities, harmonizing security incidents notification procedures at a vertical level across the Member States as well as at a horizontal level by considering different policy fields and their regulatory objectives.

4.5 CONCLUSIONS AND RECOMMENDATIONS

The adequate level of cybersecurity and resilience of medical devices is one of the crucial elements for maintaining the daily provision of health care services. Above all, it is pivotal to mitigate risks relating to patients' health and safety. On the one hand, the ongoing debate on the topic in the United States and, more recently in the European Union, shows an increasing level of awareness amongst regulators, manufacturers, health care professionals, and other involved stakeholders. On the other hand, the research presented in this chapter shows that the existing EU legal framework dealing with medical devices' cybersecurity brings significant regulatory challenges. In order to provide a step forward in mitigating these challenges, the EU regulator might consider the following recommendations:

1. Establish a more robust connection of the MDCG Guidance with EU cybersecurity (hard) laws, especially the CSA and its definitions of cybersecurity, security-by-design, and security-by-default. Ensuring consistent use of terminology across different pieces of legislation (binding and non-binding) would

[72] According to NISD, art. 4(1)(7), a security incident is an event having an actual adverse effect on the security of network and information systems. Such an event, if it involves the processing of personal data, could also qualify as a "personal data breach" (cfr GDPR, art. 4(1)(12). Finally, a security incident could also be a "serious incident" under the MDR meaning art. 4(1)(54), for instance, when the incident directly or indirectly leads to a serious public health threat, or the death of a patient. See MDCG Guidance, Annex II (examples of cybersecurity incidents/serious incidents).

[73] Including health care providers, when considered as "operators of essential services," according to NISD (art. 4(1)(4)).

[74] See COCIR, supra note 52, at 8.

[75] Id.

https://doi.org/10.1017/9781108975452.005 Published online by Cambridge University Press

also help manufacturers in meeting the requirements as it would bring more clarity in the interpretation of the MDR cybersecurity-related provisions.

2. Clarify the meaning and implications of "joint responsibility" in the intertwining with other applicable laws (in particular when it comes to the NISD, GDPR, and CSA). Further explanations on how exactly the responsibility stemming from one piece of legislation applicable to a specific stakeholder is influenced or conflicted with the responsibility of another stakeholder (stemming from the same or different piece of legislation) would represent a meaningful tool to guide manufacturers in complying with all the relevant laws.
3. Clarify the scope of application of the CSA for certification mechanisms and MDR security requirements. In particular, the EU regulator should explain how the MDR cybersecurity-related requirements apply to an ICT product which also falls under a definition of a medical device, and what type of certification schemes would be relevant.
4. Provide guidance on the application of the RED, its interaction with the MDR and other laws applicable to the cybersecurity of medical devices.
5. Ensure cooperation between competent national authorities (i.e., for incident notifications) in order to achieve timely respect of the requirements, and to avoid compliance duplication.

https://doi.org/10.1017/9781108975452.005 Published online by Cambridge University Press