PART II

European Regulation of Medical Devices Introduction

Timo Minssen

Similar to the United States' Food and Drug Administration (FDA), regulators in other jurisdictions also seek to address the increasing significance of data-driven digital health products and their interface with medical AI and machine learning. This also holds true for the European Union (EU) and its member states, as well as the United Kingdom. To be lawfully marketed within the European Union, all medical devices and in vitro diagnostic medical devices must meet the CE marking requirements under the relevant EU regulatory frameworks.[1] On May 25, 2017, two major regulatory changes simultaneously entered into force, which are highly relevant for medical device manufacturers: EU Regulation 2017/745 on medical devices (MDR) and EU Regulation 2017/746 on in vitro diagnostic medical devices (IVDR).[2] In reaction to the COVID-19 pandemic's impact on medical device stakeholders, and with patient health and safety as a guiding principle, the application date for the EU Medical Device Regulation (2017/745) (MDR) had been postponed from May 2020 to May 2021.[3] This decision was met with a sigh of relief since it gave stakeholders more time to prepare for – and comply with – the new regulatory framework. However, in light of new technical developments and capabilities many uncertainties and challenges remain to be addressed.

As the contributions in this part demonstrate, this also concerns the broader legislative framework within which the European medicine agencies and the so-called notified bodies will have to operate. In addition to product-specific regulations, these authorities will have to consider a great number of recent laws, guidance documents, policy papers, strategy announcements, and initiatives, such as the

[1] Timo Minssen et al., Regulatory Responses to Medical Machine Learning, 7 Journal of Law the Biosciences (2020), https://doi.org/10.1093/jlb/lsaa002.

[2] See Regulation 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], art. 20, O.J. (L 117/1) (EU) [hereinafter MDR]; see also Regulation 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], art. 18, O.J. (L 117/176) (EU) [hereinafter IVDR].

[3] See Commission postpones application of the Medical Devices Regulation to prioritize the fight against coronavirus, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_589.

European Health Data Space (EHDS). They will have to deal with a broad variety of relevant topics ranging from health data protection, social justice, and cybersecurity to liability, competition law, and intellectual property rights. These interacting initiatives are expected not only to have a major impact on the specific regulation, but also on the wider governance of medical devices and health data uses. To achieve the most beneficial outcome for patients and to alleviate potential risks, it is important to consider these developments from a holistic perspective. After all, most systems are only as strong as their weakest link in both regional and international contexts.

That this holds particularly true in the cybersecurity context is highlighted by Elisabetta Biasin and Erik Kamenjasevic's chapter, "Cybersecurity of Medical Devices: Regulatory challenges in the European Union." In light of recent cyber-attacks on digital hospital systems and medical devices, which has also become a major issue during the COVID-19 pandemic, their chapter delivers an important contribution to the laws of medical devices and cybersecurity. In particular, the authors analyze and discuss the interface of the EU medical devices' legal framework with the EU cybersecurity policy objectives. Highlighting a great number of recent threats and challenges, the authors conclude that "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." In order to provide a step forward in mitigating these challenges, the authors provide several recommendations that EU regulators should consider, ranging from better guidelines on specific security standards to improving the cooperation between competent national authorities.

This certainly also applies to the health data protection context, as it is explained by Hannah van Kolfschooten in the next chapter, "The mHealth Power Paradox: Improving Data Protection in Health Apps through Self-Regulation in the European Union." The author asks, "whether and to what extent self-regulation by app stores may contribute to the level of health data protection in the European Union?" To answer this question, she explores health data protection issues regarding mHealth apps, and analyzes the EU legal framework governing mHealth apps. Concentrating on the most relevant stipulations of the EU's General Data Protection Regulation (GDPR),[4] the author discusses the "benefits and risks of industry self-regulation as an alternative means to protect data protection rights in light of current mHealth regulation practices by Apple's App Store and Google's Google Play." This allows her to propose several improvements to self-regulation in this field.

The GDPR is also at the center of the next chapter by Janos Meszaros, Marcelo Corrales Compagnucci and the author of this introduction. In their chapter, "The

[4] Regulation 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) 4.5, 1–88 (EU).

Interaction of the Medical Device Regulation and the GDPR: Do European Rules on Privacy and Scientific Research Impair the Safety and Performance of AI Medical Devices?," the authors analyze a variety of GDPR stipulations on deidentification and scientific research that help "research organizations to use personal data with fewer restrictions compared to data collection for other purposes." Under these exemptions, organizations may process specific types of data for a secondary purpose without consent. However, the authors admonish the definition and legal requirements of scientific research that differ among EU Member States. Since the new EU Medical Device Regulations 2017/745 and 2017/746 require compliance with the GDPR, they argue that this legal uncertainty "might result in obstacles for the use and review of input data for medical devices," and call for "more harmonized rules, to balance individuals' rights and the safety of medical devices."

Next, Barry Solaiman and Mark Bloom consider a topic that has become increasingly important in recent years: "AI, Explainability, and Safeguarding Patient Safety in Europe: Towards a Science-Focused Regulatory Model." Their chapter examines "the efforts made by regulators in Europe to develop standards concerning the explainability of artificial intelligence (AI) systems used in wearables." Recent attempts by governments to monitor and contain the spread of the COVID-19 pandemic has certainly accelerated the increasingly invasive use of such wearables and hence the need for such standards. The authors also point out that "one key challenge for scientists and regulators is to ensure that predictions are understood and explainable to legislators, policymakers, doctors, and patients to ensure informed decision making." Examining the operation of AI networks, the authors welcome a series of recent UK and EU guidelines for such networks and applications. But they also point out that those guidelines will ultimately be restricted by the available technology. The authors therefore argue that European legislators and regulators should spend more efforts on developing minimum standards on explainability of such technologies, which should be "leveled-up progressively as the technology improves." Acknowledging the need for appropriate human oversight and liability, they contend that those standards should be "informed by the computer science underlying the technology to identify the limitations of explainability," and that "the technology should advance to help them decipher networks intelligibly."

Finally, Helen Yu's chapter "Regulation of Digital Health Technologies in the European Union: Intended versus Actual Use," focuses on "how the classification rules and postmarket surveillance system provisions of the EU Medical Devices Regulation (MDR) need to anticipate and address the actual use of DHTs." She warns that courts and regulators have so far not been "consistent on the circumstances under which manufacturers are held responsible for known or encouraged 'misuse' of their products." She therefore stresses the importance of adequately addressing "the potential harm caused to consumers who use digital health technologies (DHTs) beyond the manufacturer's intended purpose" and highlights the

"need for a framework to re-classify and regulate DHTs based on evidence of actual use."

Overall, the authors' contribution in this section demonstrates clearly how the EU and US regulators, legislators, developers, and users of medical devices are facing very similar challenges. This applies to both the micro level – with regard to the evaluation of particular medical devices – as well as on the macro level concerning the wider legal frameworks and ramifications that are so very important for the safe and efficient functioning of such devices. However, it was also shown that some aspects of the various attempts to address these and to reach acceptable trade-offs with regard to safety, efficacy, privacy, and other values differ across the pond. Against this background and considering the great variety of opportunities and risks in the increasingly complex value chains of modern medical devices, it seems more important than ever to improve international collaboration in the area and to align regulatory and legislative approaches across the globe.