6

The 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?

Janos Meszaros, Marcelo Corrales Compagnucci, and Timo Minssen

Stipulations on deidentification and scientific research in the European General Data Protection Regulation (GDPR) help research organizations to use personal data with fewer restrictions compared to data collection for other purposes. Under these exemptions, organizations may process specific data for a secondary purpose without consent. However, the definition and legal requirements of scientific research differ among EU Member States. Since the new EU Medical Device Regulations 2017/745 and 2017/746 require compliance with the GDPR, the failure to come to grips with these concepts creates misunderstandings and legal issues. We argue that this might result in obstacles for the use and review of input data for medical devices. This could not only lead to forum shopping but also safety risks. The authors discuss to what extent scientific research should benefit from the research exemption and deidentification rules under the GDPR. Furthermore, this chapter analyzes recently released guidelines and discussion papers to examine how input data is reviewed by EU regulators. Ultimately, we call for more harmonized rules to balance individuals' rights and the safety of medical devices.

6.1 INTRODUCTION

Artificial intelligence (AI) and big data have a significant impact on society,[1] as many aspects of our lives have become subject to data processing.[2] This "datafication" has

Acknowledgement: This research is supported by a Novo Nordisk Foundation grant for a scientifically independent Collaborative Research Program in Biomedical Innovation Law (grant agreement number NNF17SA0027784).

[1] Marcelo Corrales Compagnucci, Big Data, Databases and 'Ownership' Rights in the Cloud 4, 38, 40 (2020); Marcelo Corrales & Paulius Jurčys, Nudging Cloud Providers through Intermediary Services in New Technology, Big Data and the Future of Law, 154–5 (Marcelo Corrales et al. eds., 2017).

[2] Viktor Mayer-Schönberger & Kenneth Cukier, Big Data: A Revolution that Will Transform How We Live, Work, and Think (Mariner Books ed., 2013).

https://doi.org/10.1017/9781108975452.007 Published online by Cambridge University Press

also led to a rapid transformation in the delivery of health care services.[3] The new generation of medical devices represents one example of technological advance that could substantially protect and improve public health.[4] Many of these rely heavily on data and AI algorithms to prevent, diagnose, treat, and monitor sources of epidemic diseases.[5]

Though opening a world of new opportunities, rapid advances in AI medical devices have resulted in a number of highly complex dilemmas, tradeoffs, and uncertainties regarding the applicability and appropriateness of the current legal framework. Many of these legal and ethical issues relate to privacy and data protection. The European General Data Protection Regulation (GDPR)[6] is of particular importance in that respect. Focusing on the GDPR, the following chapter discusses the risk that AI medical device systems may run afoul of sufficiently informed consents of data subjects since they collect, process, and transfer sensitive personal data in unexpected ways without giving adequate prior notice, choices of participation, and other options.[7] At the same time, such data can be important to ensure the safety and effectiveness of such devices. Considering the consequential need for reasonably sound tradeoffs, we argue that current legal frameworks and definitions need to be harmonized and refined. We refer to the typical lifecycle in the collection and processing of health data via medical devices (Section 6.2) to highlight the challenges and legal risks at each phase. Section 6.3 examines the new EU regulations for Medical Devices (MDR)[8] and In Vitro Diagnostic Medical Devices (IVDR)[9] with a special focus on the MDR. In this section, we seek in particular to identify and iron out the missing links between the GDPR and the MDR.

[3] Alessandro Blasimme & Effy Vayena, Towards Adaptive Governance in Big Data Health Research: Implementing Regulatory Principles (Oct. 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3501545; Marcelo Corrales Compagnucci, Big Data, Databases and 'Ownership' in the Cloud 4, 39, 40, 299 (2019).

[4] Ugo Pagallo et al., The Rise of Robotics & AI: Technological Advances and Normative Dilemmas 1–13 (2018).

[5] Marcelo Corrales Compagnucci et al., Homomorphic Encryption: The Holy Grail for Big Data Analytics and Legal Compliance in the Pharmaceutical and Healthcare Sector, 3 EPLR 144, 145–55 (2019).

[6] 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) (Text with EEA relevance), 2016 O.J. (L 119) 4.5, at 1–88 (EU) [hereinafter GDPR].

[7] Timo Minssen et al., The EU-US Privacy Shield Regime for Cross-Border Transfers of Personal Data Under the GDPR: What Are the Legal Challenges and How Might These Affect Cloud-Based Technologies, Big Data, and AI in the Medical Sector?, 4 EPLR 34, 34–50; Marcelo Corrales Compagnucci et al., Lost on the High Seas without a Safe Harbor or a Shield? Navigating Cross-Border Data Transfers in the Pharmaceutical Sector after Schrems II Invalidation of the EU-US Privacy Shield, 4 EPLR 153, 153–160.

[8] 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 O.J. (L 117) 5.5, at 1–175 (EU) [hereinafter MDR].

[9] 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 O.J. (L 117) 5.5, at 176–332 (EU) [hereinafter IVDR].

https://doi.org/10.1017/9781108975452.007 Published online by Cambridge University Press

Section 6.4 discusses our main findings and summarizes recommendations. This provides the basis for our conclusions in Section 6.5.

6.2 COLLECTION AND PROCESSING OF HEALTH DATA UNDER THE GDPR

Modern health care systems and medical devices collect and process vast amounts of data, which may enhance an individual's health care experience directly and indirectly through scientific research and policy planning. Nevertheless, obtaining informed consent[10] or authorization from a large number of data subjects can be challenging and result in disproportionate cost and effort.[11] For instance, the Italian government provided the health data[12] of 61 million Italian citizens to IBM Watson Health, without obtaining patient consent.[13] The agreement between the Italian government and IBM underlined that IBM alone would retain rights to the results of the research, which it could then license to third parties.[14] Instead of acquiring consent for the secondary processing, the most realistic option for privacy protection is providing the option to opt-out for the citizens, such as the national data opt-out system[15] in England.[16]

In general, the processing of sensitive data (e.g., health data) is prohibited under the GDPR. This can be a crucial issue in the case of AI-augmented medical devices since the sensitivity and specificity of an algorithm are only as good as the data that they are trained on. For instance, if an algorithm is only trained on the genetic material derived from European Caucasians, it may not provide accurate information that can be generalized to individuals of other groups. However, the GDPR enables the processing of sensitive data for public interest, public health, and scientific research purposes, if there are appropriate safeguards for the rights and freedom of individuals. While the GDPR does not fully specify what those

[10] Consent is defined by GDPR, art. 4(11), as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

[11] Paul R. Burton et al., Policies and Strategies to Facilitate Secondary Use of Research Data in the Health Sciences, 46 International Journal of Epidemiology 1732, 1732–3 (2017).

[12] The health data included demographic data; all medical conditions, diagnoses, and their treatment; emergency and other hospital visits, including dates and times; prescriptions and their costs; genomic data and information about any cancers; and much else besides.

[13] Elad Leshem, IBM Watson Health AI gets access to full health data of 61m Italians, Medium (Jan. 18, 2018), https://medium.com/@qData/ibm-watson-health-ai-gets-access-to-full-health-data-of-61m-italians-73f85d90f9c0.

[14] Glyn Moody, Detailed Medical Records of 61 Million Italian Citizens to Be Given to IBM for Its "Cognitive Computing" System Watson, Privacy News Online (May 22, 2017), www.privateinternetaccess.com/blog/detailed-medical-records-61-million-italian-citizens-given-ibm-cognitive-computing-system-watson/.

[15] NHS Digital, National Data Opt-out, https://digital.nhs.uk/services/national-data-opt-out.

[16] Janos Meszaros & Chih-Hsing Ho, Building Trust and Transparency? Challenges of the Opt-Out System and the Secondary Use of Health Data in England, 19 Med. L. Int'l 159, 159–81 (2019).

https://doi.org/10.1017/9781108975452.007 Published online by Cambridge University Press

safeguards are, it indicates that their purpose is to "ensure that technical and organizational measures are in place in order to ensure respect for the principle of data minimization."[17] Such measures may include de-identification methods (for example, anonymization and pseudonymization) provided that the intended use of the data can still be fulfilled. However, differing requirements of national laws toward the application of these exemptions and de-identification methods often hinder the application of AI medical devices at the EU level. In Sections 6.2.1–6.2.3, we consider the most salient problems.

6.2.1 *Public Interest and Public Health*

Public interest and public health can be a legal basis for the secondary use of health data. The GDPR posits several levels of public interest, such as general and important.[18] However, the level of public interest in AI medical devices is still not clear and may fall under different categories. This could create problems to identify whether personal data might be processed with or without consent to develop and update these devices. Deciding on the level of public interest is as challenging as it is relevant. Medical devices need to be safe and reliable. Malfunctions could potentially cost lives. Therefore, the public interest and public health could be linked to the intended use and classification of these devices.

6.2.2 *Scientific Research*

There are situations when data was not collected for research or health care purposes initially. For instance, when a smartwatch measures a wearer's heart rate. This data can be useful later for research purposes, to find unseen correlations. The collected data provides valuable information for future research but reaching users for getting their approval for the secondary purpose would pose a significant burden, if it is possible at all. This can lead to controversial scenarios, such as the Google DeepMind[19] case in the United Kingdom, where the Royal Free Hospital under the National Health Service (NHS)[20] provided the personal data of 1.6 million patients to Google DeepMind without their consent. Google's AI medical device was an app, which could monitor an acute kidney injury disease. The app called "Streams" was used as part of a trial to test, diagnose, and detect the disease. Public

[17] GDPR, art. 89(1).

[18] Janos Meszaros & Chih-Hsing Ho, Big Data and Scientific Research: The Secondary Use of Personal Data Under the Research Exemption in the GDPR, *Acta Juridica Hungarica* 403, 403–19 (2018).

[19] DeepMind Technologies is a British artificial intelligence company founded in 2010, currently owned by Google through Alphabet Inc.

[20] Royal Free is one of the largest health care providers in Britain's publicly funded National Health Service.

https://doi.org/10.1017/9781108975452.007 Published online by Cambridge University Press

concerns and corroborative research suggested that Google DeepMind failed to comply with the provisions enshrined by data protection law.[21]

The GDPR aims to ease the restrictions on the processing of sensitive data by explicitly allowing the processing for research purposes. To use this legal basis, the data controllers need to apply appropriate safeguards (e.g., pseudonymization and anonymization) under EU and Member State laws.[22] The GDPR defines scientific research in a broad manner, which includes "technological development and demonstration, fundamental research, applied research and privately funded research" conducted by both public and private entities.[23] However, the definition of research can be found in the Recitals[24] of the GDPR, which are not legally binding by themselves. Several EU Member States, such as Germany and Finland, do not define "scientific research" in their laws. Instead, these States define the limits and requirements of research through the regulation of their authorities responsible for this field.[25] Other Member States such as Austria regulate scientific research by referring to the OECD's Frascati Manual.[26,27] The OECD Frascati Manual includes definitions of basic concepts, data collection guidelines, and classifications for compiling research and development statistics. However, the Frascati Manual never defines "scientific research" as such, even though it makes use of the term in a number of instances throughout the text. Furthermore, the application of the research exemption can lead to different interpretations. For instance, in Ireland, the application of the research exemption by the Health Research Consent Declaration Committee is significantly stricter than in the United Kingdom, by the Medical Research Council.[28] Hence, the Member States need to restrict the scope of scientific research, since overly broad interpretations might undermine the goals of the GDPR. These diverse rules on data collection pose hurdles for improving the safety of medical devices, since processing new data for updating is crucial, and the different requirements and barriers in Member States undermine the

[21] Janos Meszaros et al., Nudging Consent and the New Opt-Out System to the Processing of Health Data in England, in Legal Tech and the New Sharing Economy, 61, 68 (Marcelo Corrales Compagnucci et al. eds., 2019).

[22] GDPR, art. 9(2)(j).

[23] GDPR, Recital 159.

[24] In EU law, Recitals are usually placed at the beginning of the legal text. They introduce the legislation and explain the reasons for the provisions and clarify legislative goals. Recitals are normally not binding as such. Recitals may, however, influence interpretations of the law by Courts or further legislation and may in that way achieve binding effect.

[25] See, e.g., German Research Foundation requirements for funding scientific research, www.dfg.de/en/research_funding/principles_dfg_funding/index.html.

[26] Organisation for Economic Co-operation and Development (OECD), Frascati Manual: Guidelines for Collecting and Reporting Data on Research and Experimental Development (2015).

[27] 515th Regulation on Research, Austria, www.ffg.at/sites/default/files/downloads/service/forschungspraemienverordnung_bgbla_2012_ii_515.pdf.

[28] Mary Donnelly & Maeve McDonagh, Health Research, Consent and the GDPR Exemption (Apr. 2, 2019). This is a pre-edited version of M. Donnelly & M. McDonagh Health Research, Consent and the GDPR Exemption, 26 Eur. J. Health L. 97, 97–119 (2019).

https://doi.org/10.1017/9781108975452.007 Published online by Cambridge University Press

collection of reliable and diverse datasets. Germany's new Digital Healthcare Act[29] is a good example of promoting the use of low-risk medical devices and ensuring better usability of health data for research purposes. The Act entitles persons covered by statutory health insurance to benefit from digital health applications and contains provisions to make demographic data from health insurers more usable for research purposes.[30]

6.2.3 *Deidentification*

Deidentification methods represent a broad spectrum of tools and techniques to protect the data subject's privacy. In general, the strength of the deidentification scales with a loss in data utility and value.[31] The two ends of this spectrum are clear: personal data without any deidentification, which can directly identify the data subject and anonymous data, which cannot identify individuals.[32] Between these two ends, there is a wide range of methods and techniques, which need further clarification. The GDPR clarifies that pseudonymized data is a type of personal data.[33] However, the definition of pseudonymization is too broad to know the requirements to reach an adequate level of deidentification. Recognizing the broad spectrum of deidentification techniques and acknowledging them as an "appropriate safeguard" enables the development of regulatory guidance that encourages the maximum use of deidentification, and it may open the door for the safe secondary use of data in scientific research.

Public interest, public health, and scientific research represent a broad exemption from the prohibition of the processing of sensitive data in the GDPR. These legal bases also require safeguards, such as deidentification techniques. However, the application of them in the Member States is not unified. This may trigger

[29] Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz – DVG) [Digital Healthcare Act] of 9 December 2019, BGBl I at 2562 (Germany, 2019). Compare also Germany's new Hospital Future Act, Gesetz für ein Zukunftsprogramm Krankenhäuser (Krankenhauszukunftsgesetz – KHZG), G. v. 23.10.2020 BGBl. I S. 2208 (Nr. 48).

[30] Sara Gerke et al., Germany's Digital Health Reforms in the COVID-19 Era: Lessons and Opportunities for Other Countries, 3 npj Digit. Med. 94 (2020).

[31] Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA L. Rev. 1706 (Aug. 13, 2009); U. of Colorado Law Legal Studies Research Paper No. 9–12, https://ssrn.com/abstract=1450006.

[32] The GDPR has strict expectations towards anonymization. Unlike the Health Insurance Portability and Accountability Act (HIPAA) in the United States, which sets forth a rule exempting data from regulation if eighteen specific identifiers are removed, the GDPR applies the standard that data is anonymous only when it cannot be identified by any means by any person (GDPR, Recital 26).

[33] However, many scholars are challenging the idea that pseudonymized data constitutes personal data in all cases. For instance: Miranda Mourby, Elaine Mackey, Mark Elliot, et al., Are "Pseudonymised" Data Always Personal Data? Implications of the GDPR for Administrative Data Research in the UK, 34 (2) *Computer Law and Security Review* 222–33 (2018); Anne Bahr & Irene Schlünder, Code of Practice on Secondary Use of Medical Data in European Scientific Research Projects, 5 *International Data Privacy Law* 279, 279–91 (2015).

https://doi.org/10.1017/9781108975452.007 Published online by Cambridge University Press

unnecessary legal risks in the development and deployment of AI medical devices and takes us directly to what has been called the "update problem":[34] how can regulators, as well as reliable developers and producers, determine when the updated AI behaves differently enough that a new assessment is needed? It is challenging to ensure that AI medical devices conform to all the rules and technical issues without posing new risks than those assessed during the premarket review.[35] Considering that the essence of updating medical devices potentially introduces new risks without constant approval, it is crucial to validate the data they are learning from. Therefore, regulators and product manufacturers need to implement a risk reassessment and incident-report framework, which includes ongoing evaluation and mitigation strategies throughout the whole lifecycle of AI medical devices, in particular, during service deployment and operation phases. For this, harmonized rules on the collection and processing of health data as well as review systems and processes of medical devices would be necessary in the EU Member States.

6.3 THE EU MEDICAL DEVICE REGULATION

To keep up with advances in science and technology, two new EU regulations on medical devices and in vitro diagnostic medical devices entered into force on May 25, 2017.[36] They will progressively replace the existing directives[37] after a staggered transitional period.[38]

The MDR clarifies that data protection rules need to be applied when medical devices process personal data.[39] Therefore, if a medical device regulated by the MDR collects personal data, it also falls under the GDPR. The MDR differentiates among three classes of medical devices, depending on their level of risk:

1. Class I devices, posing low/medium risk (e.g., wheelchairs);
2. Class IIa and IIb devices, representing medium/high-level risk (e.g., x-ray devices);

[34] B. Babic et al., Algorithms on Regulatory Lockdown in Medicine. Prioritize Risk Monitoring to Address the "Update Problem," 366 Science 1202, 1202–4 (2019).

[35] Glenn Cohen et al., The European AI Strategy: Implications and Challenges for Digital Health (forthcoming LANCET-Digital Health).

[36] Supra notes 9 & 10.

[37] Council Directive 90/385/EEC on Active Implantable Medical Devices (AIMDD) (1990); Council Directive 93/42/EEC on Medical Devices (MDD) (1993); Council Directive 98/79/EC on in vitro Diagnostic Medical Devices (IVDMD) (1998).

[38] The Council and the Parliament adopted on 23 April 2020 Regulation 2020/561 amending Regulation 2017/745 on medical devices regarding application dates of certain of its provisions. This Regulation postpones the date of application for most Medical Devices Regulation provisions by one year – until 26 May 2021. This postponement alleviates the pressure off national authorities, notified bodies, manufacturers, and other actors so they can focus fully on urgent priorities related to the COVID-19 crisis. The IVDR Regulation 2017/746 corresponding date of application remains the same (May 2022).

[39] Regulation 2017/745 Recital 47, arts. 62(4)(h), 72(3), 92(4), 110(1)–(2) (EU).

https://doi.org/10.1017/9781108975452.007 Published online by Cambridge University Press

3. Class III, high-risk devices (e.g., pacemakers).

In the case of low-risk level (Class I) medical devices, such as a smartwatch, privacy might often prevail over the secondary use of personal data to develop and improve these devices. In the case of high-risk level (Class III), the safety of medical devices might outweigh patient privacy. AI medical devices with a medium risk level (Class II), such as medical image processing software, may be considered to have at least a general level of public interest. However, developing high-risk devices does not mean that manufacturers could automatically process health data without consent. Careful consideration is necessary on a case-by-case basis with strong safeguards, under the oversight of authorities.

Medical devices in the European Union need to undergo a conformity assessment to demonstrate that they meet legal requirements. The conformity assessment usually involves an audit of the manufacturer's quality system and, depending on the type of device, a review of technical documentation from the manufacturer on the safety and performance of the device.[40] Manufacturers can place a CE (Conformité Européenne) mark on their medical device after passing the assessment. The EU Member States can designate accredited notified bodies to conduct conformity assessments. A notified body within the European Union is an entity designated by an EU competent authority to assess the conformity of medical devices before being placed on the market. Companies are free to choose the notified body they engage with.[41] There are more than fifty EU notified bodies in total that can certify according to Medical Device Directives. However, not all of these notified bodies can certify according to all categories of medical device products. When the authorities start to scrutinize the AI/ML medical device during the approval process, it is challenging to know clearly how the AI application and algorithms developed and evolved due to their opaque nature.[42] It is not clear how notified bodies can review the input data of AI medical devices. First, reviewing large and complex datasets requires special knowledge and technical expertise, which might be lacking or not at the same level within all the notified bodies of the European Union. Second, there are medical devices developed outside of the European Union. Reviewing the datasets used for developing them might trigger data protection and data transfer jurisdictional issues. The datasets might contain sensitive data of individuals from countries outside Europe, thus data sharing is challenging, posing a hurdle for part of the review process. For instance, the Health Insurance Portability and Accountability Act (HIPAA) and state regulations in the

[40] EMA, Medical devices, www.ema.europa.eu/en/human-regulatory/overview/medical-devices.

[41] European Medicines Agency, Questions & Answers on Implementation of the Medical Devices and In Vitro Diagnostic Medical Devices Regulations, ((EU) 2017/745 and (EU) 2017/746) (Oct. 21, 2019) Rev.1 EMA/37991/2019.

[42] US Food & Drug Admin., Executive Summary for the Patient Engagement Advisory Committee Meeting, Artificial Intelligence (AI) and Machine Learning (ML) in Medical Devices (Oct. 22, 2020). William Nicholson Price II, Regulating Black-Box Medicine, 116 Mich. L. Rev. 421 (Mar. 21, 2017).

https://doi.org/10.1017/9781108975452.007 Published online by Cambridge University Press

United States, and Japanese regulations on personal data[43] might not allow the sharing of sensitive data with the notified bodies in the EU Member States. Moreover, sharing anonymized data might not be sufficient to review input data thoroughly. Third, there is a great variety of data-processing software and methods among companies operating in different countries, which makes it extremely challenging to review these devices uniformly on the same level.

The European Medicines Agency and several notified bodies are already preparing for the change of AI medical devices. The European Medicines Agency and the Heads of Medicines Agencies (HMA) Big Data Task Force (BDTF)[44] released two reports[45] recently for the European regulators and stakeholders to realize the potential of big data in terms of public health and innovation. Since the biggest issues in the European Union currently are the decentralization of health data and regulatory tasks, the reports focus on providing guidance and resources for data quality and discoverability to build up computing and analytical capacity. Thus, the most ambitious recommendation of the BDTF is the establishment of an EU platform: Data Analysis and Real World Interrogation Network (DARWIN) to access and analyze health care data from across the European Union. This platform would create a European network of databases with verified quality and strong data security. It is intended to be used to inform regulatory decision making with robust evidence from health care practice. The reports highlight the following actions for the European Union:

1. Ensuring sufficient expertise and capacities within the European network (in all the notified bodies in the Member States), in order to ensure that AI medical devices can be assessed appropriately.
2. Enable regulatory evaluation of clinical data submitted by drug manufacturers for approval where the data has been processed by AI algorithms or if part of the analysis, such as patient selection, involved AI methods.
3. Enable regulatory use of AI in internal processes at authorities and notified bodies. For instance, applying Natural Language Processing of received texts, or reviewing image data submitted to support a clinical claim from a drug manufacturer.
4. Approval of AI-based Health Apps in devices intended for clinical decision making.

The reports also clarify that the European Union cannot accept opaque algorithms performing without checks and balances. Algorithm code should be

[43] Act on the Protection of Personal Information (Act No. 57 of May 30, 2003, as amended, APPI).

[44] The HMA/EMA Task Force on Big Data was established in 2017 to report on the challenges and opportunities posed by big data in medicine regulation.

[45] See, e.g., HMA-EMA Joint Big Data Taskforce Phase I and Phase II reports on “Evolving Data-Driven Regulation” (2019), www.ema.europa.eu/en/documents/other/hma-ema-joint-big-data-taskforce-phase-ii-report-evolving-data-driven-regulation_en.pdf.

https://doi.org/10.1017/9781108975452.007 Published online by Cambridge University Press

more transparent (feature selection, code, original data set) and available for targeted review by regulators and notified bodies. The report states that the outcomes and changes to algorithm use (safety and efficacy) need to be subject to post-marketing surveillance mechanisms, in a similar way as monitoring drug safety after marketing authorization. By way of comparison, the European Union's approach for the assessment of medical devices is slightly different from the FDA's in the United States. While the reports suggest that the European Union is still focusing on the transparency of AI applications, the FDA also pays special attention to the excellence and trustworthiness of the companies developing AI medical devices during the precertification process.[46] Figure 6.1 below shows the flow of health data for developing AI medical devices in the European Union.

6.4 DISCUSSION

The effective collection and processing of relevant health data is the first step to making AI medical devices that work properly. This is particularly relevant during the COVID-19[47] outbreak as the foreseeable reuse of health data for scientific purposes leads to a rise in the number of organizations manufacturing AI medical devices.[48] The US Sentinel system is a great example of monitoring the safety of medical devices and securely sharing and reusing the collected information.[49] Our analysis suggests, however, that the processing and review of input data for medical devices, as well as the definition of specific data uses, are not fully harmonized in the European Union. This issue stems from the fact that the health care systems and scientific research are mainly regulated by the EU Member States, resulting in diverse legal environments and barriers for processing health data. Thus, the GDPR and Medical Device Regulation have not reached a sufficient level of harmonization in this field. This may result in unnecessary legal risks in the development and deployment of AI medical devices, which is crucial in the case of the "update problem."[50] Therefore, harmonized rules on the collection and processing of health data, as well as review systems and processes of medical devices, would be necessary in the EU Member States.

[46] US Food & Drug Admin., Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) – Discussion Paper and Request for Feedback (2019).

[47] Guidelines 04/2020 on the use of location data and contact tracing tools in the context of COVID-19 outbreak adopted on 21 April 2020.

[48] European Data Protection Supervisor, A Preliminary Opinion on Data Protection and Scientific Research (Jan. 6, 2020), https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf.

[49] US Food & Drug Admin., FDA's Sentinel Initiative, https://www.fda.gov/safety/fdas-sentinel-initiative (Nov. 26, 2020).

[50] B. Babic et al., Algorithms on Regulatory Lockdown in Medicine. Prioritize Risk Monitoring to Address the "Update Problem," 366 Science 1202, 1202–4 (2019).

https://doi.org/10.1017/9781108975452.007 Published online by Cambridge University Press

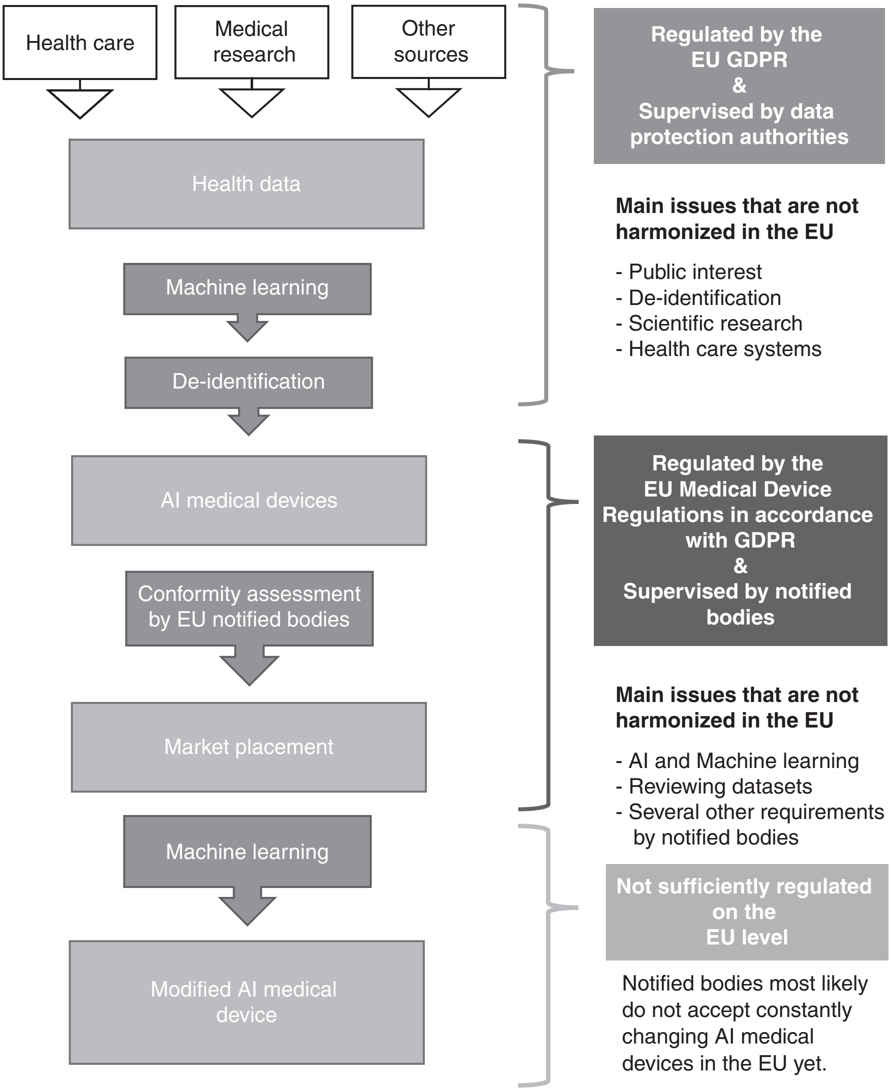
Health care
Medical research
Other sources
Health data
Machine learning
De-identification
AI medical devices
Conformity assessment by EU notified bodies
Market placement
Machine learning
Modified AI medical device
Regulated by the EU GDPR & Supervised by data protection authorities
Main issues that are not harmonized in the EU
- Public interest
- De-identification
- Scientific research
- Health care systems
Regulated by the EU Medical Device Regulations in accordance with GDPR & Supervised by notified bodies
Main issues that are not harmonized in the EU
- AI and Machine learning
- Reviewing datasets
- Several other requirements by notified bodies
Not sufficiently regulated on the EU level
Notified bodies most likely do not accept constantly changing AI medical devices in the EU yet.

FIGURE 6.1. The processing of health data for developing AI medical devices

The "update problem" is still not sufficiently addressed and little work has thoroughly examined how AI medical devices are developed and built from the perspectives of public interest and data protection law. To build these devices, data-intensive research is necessary. However, at what cost? Strong privacy protection may hinder the development, effectiveness, and precision of AI products and services. Globally, there is a drive to create competitive pharmaceutical and health care industries. As a result, the developers of AI medical devices and

https://doi.org/10.1017/9781108975452.007 Published online by Cambridge University Press

services have enjoyed a privileged position since they have been able to further use health data with less restrictions, and sometimes without adequate consent.[51] On the one hand, this could save lives and minimize treatment costs.[52] An increased precision due to better and more data, might even help to identify, monitor, and correct potential risks for bias in the data. On the other hand, this situation might lead to the further use of sensitive data with less control and increasing risks for privacy breaches.

To address this dilemma and achieve reasonable tradeoffs, we suggest the following measures to advance the assessment of the safety and efficacy of AI medical devices in the European Union. First, we believe that the expected level of public interest in the case of the secondary use of health data for developing AI medical devices must be clarified for different categories of medical devices, considering both the intended and unintended use scenarios.[53] Second, we propose to regulate the definition and requirements of scientific research on the EU level to harmonize the secondary use of health data. This would be crucial for providing a sufficient amount of quality data for machine learning in the case of AI medical devices. Moreover, collecting personal data and processing it for a purpose with public interest should not result in a product or service that negatively affects the data subject's rights. Third, we think that more guidance would be necessary on the safeguards and expected level of de-identification on health data, without overconfidently relying on them. Fourth, we call upon the EMA and notified bodies to be properly prepared for the review of (large) datasets since it is the foundation of AI medical devices. While opening and assessing opaque algorithms is challenging for regulators, we believe that a reasonable level of transparency should be required to allow for sufficient regulatory review of medical device systems.[54] This does not necessarily imply that every single computational step must be traceable.[55] For instance, some algorithms could still be utilized to construct a transparent and trusted AI system "as long as the assumptions and limitations, operational protocols, data properties, and output decisions can be systematically examined and validated."[56] Fifth, we recommend harmonizing the conformity assessment of notified bodies to provide safety, allow for

[51] Julia Powles & Hal Hodson, Google DeepMind and Healthcare in an Age of Algorithms, 7 Health Tech. 351, 351–67 (Dec. 2017).

[52] Jonathan H. Chen & Steven M. Asch. , Machine Learning and Prediction in Medicine – Beyond the Peak of Inflated Expectations, 376 N. Engl. J. Med. 2507 (Jun. 2017).

[53] Helen Yu, Regulation of Digital Health Technologies in the EU: Intended vs Actual Use, in Future of Medical Device Regulation: Innovation and Protection (Cambridge University Press ed., Oct. 2020); see also Timo Minssen et al., When Does Stand-Alone Software Qualify as a Medical Device in the European Union? – The Cjeu's Decision in Snitem and What It Implies for the Next Generation of Medical Devices, 28 Med. L. Rev. 615, 615–24 (2020).

[54] Timo Minssen, Regulating Digital Health, Gary Humphreys Report (2020), www.who.int/bulletin/volumes/98/4/20-020420.pdf.

[55] Id.

[56] Id.

https://doi.org/10.1017/9781108975452.007 Published online by Cambridge University Press

European-wide reports on unwanted incidents, and avoid forum shopping. Sixth, and finally, we propose to develop special regulation and oversight for AI research to allow for a better coordination and compliance assessment in view of the great variety of separate regulations concerning data protection, health care, and medical research.

6.5 CONCLUSION

Harnessing the full benefits of AI-driven medical devices offers many opportunities, in particular in health crisis situations, such as the ongoing COVID-19 pandemic. However, many legal risks and lingering questions remain unsolved. The European Union does not yet have the means to fully exploit the benefits of this data due to heterogeneous health care systems with different content, terminologies, and structures.[57] In addition, the European Union currently has no pan-European data network and is lagging behind other regions in delivering answers for health care-related regulatory questions.[58] Although the GDPR and Medical Device Regulations aim to address some of these challenges by harmonizing the processing of data and risk assessment of AI medical devices in the European Union, these areas still remain diversified. To enhance the performance and safety of medical devices, it will be important to improve the dialogue between data protection authorities, ethical review boards, notified bodies, and medicine agencies. The proposed recommendations discussed in this chapter attempt to enhance this dialogue for a better understanding and alignment between the medical device sector, regulators, public research programs, and data protection standards.[59] This could form the basis for a legal debate on the circumstances under which access by researchers to health data by private companies can be justified based on public interest and research exemptions.[60] Considering the increasing importance of public-private partnerships and AI-driven medical devices proactive initiatives to that effect appear more important than ever.[61] The ongoing implementation of the EU strategies concerning AI, Data and medical innovation plays an important role in that regard. This has not only resulted in the

[57] European Medicines Agency, A Common Data Model for Europe? Why? Which? How? Workshop report from a meeting held at the European Medicines Agency 10, 10–11 (Dec. 2017), www.ema.europa.eu/en/documents/report/common-data-model-europe-why-which-how-workshop-report_en.pdf.

[58] Id. at 31.

[59] Cf. European Data Protection Supervisor, A Preliminary Opinion on Data Protection and Scientific Research, EDPS (Jan. 6, 2020), https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf.

[60] Id.

[61] Press release. Commission and Germany's Presidency of the Council of the EU underline importance of the European Health Data Space, https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2049 (Nov. 11, 2020).

https://doi.org/10.1017/9781108975452.007 Published online by Cambridge University Press

evolving formation of the European Health Data Space,[62] but also in the adoption of a new EU Data Governance Act[63] and the proposal of an AI Regulation,[64] which provides for regulatory sandboxes for low-risk devices. It is the hope of the authors that these developments will improve the current situation.

[62] Press release. Commission and Germany's Presidency of the Council of the EU underline importance of the European Health Data Space, https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2049 (Nov. 11, 2020).

[63] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (Data Governance Act)
COM/2020/767 final. Cf. www.euractiv.com/section/digital/news/data-governance-new-eu-law-for-data-sharing-adopted/.

[64] 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.

https://doi.org/10.1017/9781108975452.007 Published online by Cambridge University Press