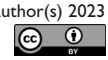
*Case Commentary*

MEDICAL LAW INTERNATIONAL

# Interoperability and governance in the European Health Data Space regulation

Medical Law International
1–9



DOI: 10.1177/096853322311656 92
journals.sagepub.com/home/mli


**Petros Terzis**
University College London, UK

**(Enrique) OE Santamaria Echeverria**
Erasmus School of Law, The Netherlands

## Abstract

The proposal for a regulation on the European Health Data Space (EHDS) is a much-awaited project. It aspires to create a harmonised framework – a common European data space – for the administration of health data (primary use) across Member States and the promotion of healthcare research and innovation (by establishing rules for the secondary use of health data). As such, although the EHDS proposal is a legal document, in its essence, it includes provisions that introduce not only legal, but also institutional, and technical-infrastructural changes. Overall, together with the Regulation 2017/745 on medical devices, the Data Governance Act (DGA), the Data Act, the AI Act, and the General Data Protection Regulation (GDPR), the EHDS proposal will complete the regulatory canvas for the use of health data in the European Union. Although we are supportive of the EHDS initiative, there are aspects of the proposal that require further debate, reconsideration, and amendments. Following previous work on potential power asymmetries encapsulated in the Proposal, in this commentary, we focus on the provisions of/for interoperability of the Electronic Health Record (EHR) systems (Ar. 14–32) as well as the provisions on the structure of Health Data Access bodies and their cross-border organisation (section 3). We recommend a series of amendments to orientate the EHDS project better to its constitutive goals: the promotion of public health research and respect for the rights of the individuals.

## Keywords

European Health Data Space, Electronic Health Records, interoperability, governance, commons

Received 8 March 2023; Revised 8 March 2023; Accepted 9 March 2023

**Corresponding author:**
Petros Terzis, Faculty of Laws, University College London, Bentham House, Endsleigh Garderns, London, WC1H 0EG, UK.
Email: petros.terzis@ucl.ac.uk

## Introduction

The proposal for a regulation on the European Health Data Space (EHDS) is a much-awaited project. It aspires to create a harmonised framework – a common European data space – for the administration of health data (primary use) across Member States and the promotion of healthcare research and innovation (by establishing rules for the secondary use of health data).[1] As such, although the EHDS proposal is a legal document, in its essence, it includes provisions that introduce not only legal, but also substantial institutional, as well as technical-infrastructural, changes. Overall, together with the Regulation 2017/745 on medical devices, the Data Governance Act (DGA), the Data Act, the AI Act, and the General Data Protection Regulation (GDPR), the EHDS proposal will complete the regulatory canvas for the use of health data in the European Union (EU).

Although we are supportive of the EHDS initiative, there are aspects of the proposal that require further debate, reconsideration, and amendments. There is an ongoing body of work on various aspects of the Proposal.[2] Following previous work on potential power asymmetries encapsulated in the Proposal, in this commentary, we focus on the provisions of/for interoperability of the Electronic Health Record (EHR) systems (Ar. 14–32) as well as the provisions on the structure of Health Data Access bodies and their cross-border organisation (section 3). We recommend a series of amendments to orientate the EHDS project better to its constitutive goals: the promotion of public health research and respect for the rights of the individuals. The proposal is currently under discussion at the Committee on Civil Liberties, Justice, and Home Affairs (LIBE) and the Committee on the Environment, Public Health, and Food Safety (ENVI), and the joint draft report is expected to be published at the end of March 2023. The commentary is based on the text of the proposal at the time of writing.

## Interoperability and privacy in the EHR systems

The Proposal introduces new rules for manufacturers of EHR systems that wish to place their products and services in the EU market, thereby complementing the

1. Proposal 2022/0140 (COD) for a Regulation of the European Parliament and the Council on the European Health Data Space, European Commission.
2. See indicatively. Tjasa Petrocnik, 'Health Data between Improving Health(Care) and Fuelling the Data Economy: Editorial', *Technology and Regulation* 2022 (2022), pp. 124–127; Petros Terzis, 'Compromises and Asymmetries in the European Health Data Space', *European Journal of Health Law* 1 (2022), pp. 1–19; André Caravela Machado and Daniel Ferreira Polónia, 'Legal and Technological Aspects for the Creation of a European Health Data Space', *2022 17th Iberian Conference on Information Systems and Technologies (CISTI)*, Madrid, Spain, 22–25 June 2022; Denis Horgan, Marian Hajduch, Marilena Vrana, Jeannette Soderberg, Nigel Hughes, Muhammad Imran Omar, Jonathan A. Lal, Marta Kozaric, Fidelia Cascini, Verena Thaler, Oriol Solà-Morales, Mário Romão, Frédéric Destrebecq, and Edith Sky Gross, 'European Health Data Space – An Opportunity Now to Grasp the Future of Data-Driven Healthcare', Healthcare 10 (2022), p. 1629; Mahsa Shabani and Sami Yilmaz, 'Lawfulness in Secondary Use of Health Data: Interplay between Three Regulatory Frameworks of GDPR, DGA & EHDS', *Technology and Regulation* 2022 (2022), pp. 128–134; Santa Slokenberga, 'Scientific Research Regime 2.0? Transformations of the Research Regime and the Protection of the Data Subject that the Proposed EHDS Regulation Promises to Bring Along', *Technology and Regulation* 2022 (2022), pp. 135–147.

existing regime established by the Regulation 2017/745 on medical devices and the Regulation (EU) 2017/746 on *in vitro* diagnostic medical devices. In particular, Articles 14–27 of the Proposal set out a self-regulatory scheme that invites manufacturers to declare their conformity with the general specifications of the Proposal and its Annex – specifications that are primarily linked to issues of interoperability and security. For instance, manufacturers of EHR systems will have to draw a declaration of conformity to the common specifications and the essential requirements laid down in Article 23 of the Proposal, its Annex, and any additional set of rules that will follow by means of implementing acts.[3] In turn, entities that wish to import or distribute EHR systems in the EU market (e.g. Apple's AppStore or Google's Play Store) will then have to verify that all relevant declarations of conformity have been made and that the required information is provided by the manufacturer. If, however, they 'consider or have reasons to believe' that an EHR system is not in conformity with the Proposal, they can delay import or distribution until the systems' parameters align with the scheme's requirements.[4]

There are two aspects of this part of the proposal that merit careful policy attention. The first relates to the interplay between interoperability and privacy, while the second revolves around Big Tech and its potential future in the EHR market.

The relationship between interoperability and health data has always been peculiar. On one hand, interoperability brings efficiency and inter-organisational alignment, but usually comes with privacy compromises, since access to health data becomes more comprehensive and longitudinal.[5] On the other hand, strong privacy protections can enable interoperability while respecting the privacy of the individuals. For example, the DP-3T team demonstrated during the Covid-19 pandemic that one can build an interoperable infectious disease exposure notification system without necessarily compromising people's privacy.[6] Yet, the issue of privacy and data protection is scarcely mentioned

3. Proposal 2022/0140 (COD) for a Regulation of the European Parliament and the Council, Ar.s 23–24 on the European Health Data Space.
4. Ibid., Ar. 19 (5).
5. See indicatively, Mark A Rothstein and Stacey A Tovino, 'Privacy Risks of Interoperable Electronic Health Records: Segmentation of Sensitive Information Will Help', *Journal of Law, Medicine & Ethics* 47 (2019), pp. 771–777; Giorgia Bincoletto, 'Data Protection Issues in Cross-Border Interoperability of Electronic Health Record Systems within the European Union', *Data & Policy* 2 (2020), p. e3; Fatemeh Rezaeibagha, Khin Than Win, and Willy Susilo, 'A Systematic Literature Review on Security and Privacy of Electronic Health Record Systems: Technical Perspectives', *Health Information Management: Journal of the Health Information Management Association of Australia* 44 (2015) 23–38; Helma van der Linden, Dipak Karla, Arie Hasman, and Jan Talmon, 'Inter-Organizational Future Proof EHR Systems: A Review of the Security and Privacy Related Issues', *International Journal of Medical Informatics* 78 (2009), pp. 141–160.
6. The problem of power and infrastructural dependency in cases where privacy is preserved thanks to proprietary standards and protocols (a scenario not unlikely in future EHDS standardisation discussions) remains out of the scope of this note, but we hope to explore it further as the EHDS initiative evolves.

in the essential requirements and common specifications for the conformity declaration of the EHR systems' manufacturers.[7]

The omission of extensive attention to privacy and data protection concerns is surprising and requires further consideration. An earlier Recommendation by the European Commission – which the Proposal explicitly acknowledges as 'the foundation' for a European EHR common framework – included provisions on 'citizen-centric' design and data protection by design and by default.[8] These principles were not included in the final text of the Proposal. Meanwhile, despite their paramount significance for data protection within inter-organisational data flows, the issues of user authorisation (i.e. who will be authorised to access what information across systems) and audit of logs (who accesses what information) are not sufficiently addressed by the Proposal's specifications.[9] Viewed alongside the provisions for the voluntary labelling of wellness applications, this omission becomes even more troubling, since Article 31 enables developers of wellness applications to achieve interoperability with EHR systems through a self-declaratory labelling scheme that would feed EHR systems with new (sources of) data (i.e. data on wellbeing and lifestyle generated by smart watches and IoT (Internet of Things) devices). As a result, what used to be a data exchange driven by the formal and informal laws of the doctor–patient relationship risks becoming a hazy landscape where information is circulated among and across systems without patients' knowledge, or implicit or explicit consent.

The Proposal puts important market considerations at stake. Big Tech companies have recently made their first steps into the EHR market in various ways. Amazon has recently partnered with One Medical to create the Amazon Clinic.[10] Meditech, an EHR vendor has announced that its systems (used by over 600 hospitals and clinics) will be integrating with Google's Care Studio for easy search and access to patients' data.[11] In parallel, Apple has partnered with two hospitals in the United Kingdom to enable patients to

7. The only reference is made in Article 23 (3) (e) which reads, 'The common specifications *may* (emphasis added) include elements related to the following: [. . .] e) requirements and principles related to security, confidentiality, integrity, patient safety and protection of electronic health data'.
8. See recital 19 of the Proposal and Commission Recommendation (EU) 2019/243 of 6 February 2019 on a European Electronic Health Record exchange format (OJ L 39, 11.2.2019).
9. See, relatedly, van der Linden and others (n 7) 152. In further complicating the issue, the Annex II (2.4.) of the Proposal reads, 'An EHR system shall not include features that prohibit, restrict or place undue burden on authorised access, personal electronic health data sharing, or use of personal electronic health data for permitted purposes'.
10. Lydia Ramsey Pflanzer, 'Amazon Has Been Trying to Break into Healthcare for Years. Here's a Look at Everything It's Done' (*Business Insider*, 30 January 2023), available at https://www.businessinsider.com/amazon-healthcare-rxpass-pharmacy-clinic-one-medical (accessed 14 February 2023).
11. 'Meditech and Google Health Collaborate to Advance Clinical Search and Discovery in Expanse EHR' (*MEDITECH*, 15 March 2022), https://ehr.meditech.com/news/meditech-and-google-health-collaborate-to-advance-clinical-search-and-discovery-in-expanse-ehr (accessed 14 February 2023).

access their medical records through iPhones.[12] Furthermore, Apple's newly added 'medication tracking' function is likely to further strengthen Apple's role in the EHR landscape.[13] At the same time, wearable devices and cloud infrastructures owned and operated by Big Tech are increasingly significant for the creation, maintenance, update, and enrichment of health records. As the interoperability project moves forward, it is likely that (voluntary) standardisation practices will benefit the incumbent systems and tools. In this context – and without disregarding the value of giving people easy access to their health records – uncritical invitation to interoperability that fails to account for market imbalances further risks exacerbating the dependency of critical public functions on Big Tech and its infrastructure.

## Commons, governance, and interoperability of the health data access bodies

Chapter IV of the Proposal is devoted to the secondary use of health data. It introduces a governance regime for health data exchanges among entities. An important pillar of this initiative (and of the Proposal overall) is the Commission's objective to create common European data spaces. Relatedly, the Proposal includes provisions on data altruism – linking its meaning and operation with those of the DGA. However, despite the repeated use of the term 'common' (i.e. 'common standards', 'commons specifications', 'common data spaces') or commons-like rhetoric (i.e. 'altruism'), it is important to differentiate the EHDS initiative from other initiatives for data commons in the healthcare sector.

Broadly defined, commons are both tangible and intangible resources that should be accessible to all members of a certain community (e.g. global, supranational, national, local). Classic examples of the tangible resources include natural resources such as water and air, while intangible resources such as knowledge, languages, and codes are the result of the production in common of (im)material wealth.[14] Knowledge commons, specifically, are a type of commons for the governance of intelligible ideas, science, information, and data.[15] The rationale behind the construction of such a commons is that, since knowledge is cumulative, building knowledge is a common good which should be accessible for present and future generations.[16] The cumulative

12. Andrew Griffin, 'Your iPhone Can Now Download Your Personal Health Information from Your Hospital' (*The Independent*, 7 October 2020), https://www.independent.co.uk/tech/apple-iphone-health-records-uk-update-hospital-oxford-milton-keynes-b866185.html (accessed 14 February 2023).
13. Nicole Wetsman, 'Apple Adds Medication Tracking Feature to the Health App' (*The Verge*, 6 June 2022), https://www.theverge.com/2022/6/6/23144267/apple-watch-health-app-sleep-medications-wwdc (accessed 14 February 2023).
14. M. R. Marella, 'The Commons as a Legal Concept', *Law and Critique* 28(1) (2017), pp. 61–86.
15. K. Strandburg, B. Frischmann, and M. Madison, 'The Knowledge Commons Framework', in K. Strandburg, B. Frischmann, and M. Madison, eds., *Governing Medical Knowledge Commons* (Cambridge University Press, 2017), p. 10.
16. C. Hesse and E. Ostrom, 'Introduction: An Overview of the Knowledge Commons', in Charlotte Hesse and Elinor Ostrom, eds., *Understanding Knowledge as a Commons. From Theory to Practice* (MIT Press direct, 2005), pp. 7–8.

characteristic of knowledge makes the governance of knowledge commons special: it encompasses both resource production and use within and beyond the commons community.[17] Moreover, unlike material commons, the boundaries of knowledge commons are often built (instead of found) using the law and legal tools.[18] (The most common example is patents).

At first glance, one might think that by imposing a duty on data holders to make several categories of health data available for secondary use,[19] the EHDS is paving the way for an authentic form of data commons. However, a closer look at the EHDS structure reveals different standards on the nature of entities that qualify as data holders (who bear obligations to share data) and as data users (who may use data collected from other sources), respectively.[20] This leaves open the possibility for data users to exploit and further enclose their data wealth. Presaging problems like this, Paul Keller and Alek Tarkowski observe while describing the 'paradox of open':

> Opening up informational resources means exposing them to the power structures governing the networked information ecosystem. As that ecosystem has become dominated by monopolistic intermediaries, it is necessary to re-examine the assumption that opening up resources predominantly results in emancipatory and empowering consequences.[21]

In terms of 'giving back to the commons', Article 46, paragraph 11, of the proposal does prescribe that data users 'shall make public the results or output of the secondary use of electronic health data'. However, it remains unclear what exactly is meant by research results. At the time of writing, amendments are being considered on this issue, particularly for the protection of the (intellectual) rights of data holders.[22] Certain questions therefore arise: Will discoveries and inventions be put in the public domain? At which stage of a clinical trial will the data become available? And which data? Will it be possible to access the clinical trial's primary data or will this be deemed an 'intellectual property' of the sponsor? What will happen when there is a conflict between the 'duty to give back' and intellectual property claims? How this obligation for 'public' will play out in the case of algorithmic tools? Would it suffice for a Big Tech company to develop, for example, an AI diagnostic tool using data from EHDS to make its output public only through an API while retaining total control over the conditions of such access?

In terms of governance, despite the use of commons-like terminology and rhetoric, the proposed structure of the Health Data Access Bodies seems at best loosely aligned

17. Strandburg et al., 'Knowledge Commons', p. 13.
18. Op. cit., p. 14.
19. Proposal 2022/0140 (COD) for a Regulation of the European Parliament and the Council, Ar. 33 (1) on the European Health Data Space).
20. Terzis, 'Compromises and Asymmetries' (n 1).
21. Paul Keller and Alek Tarkowski, 'The Paradox of Open' (*Open Future*), https://paradox.openfuture.eu/ (accessed 7 February 2023).
22. Gerardo Fortuna, 'Council Hashes out Secondary Use of Data in EU Health Data Space' (*EURACTIV*, 27 January 2023), https://www.euractiv.com/section/health-consumers/news/council-hashes-out-secondary-use-of-data-in-eu-health-data-space/ (accessed 6 February 2023).

to a knowledge commons project. This is because – in addition to asymmetries and free-riding by big market players – as 'Open Future' and 'Instrat' note on their consultation submission, the proposal is extremely vague on the democratic safeguards and accountability provisions underlying the creation of Health Data Access bodies.[23] As it stands, processing to create or to acknowledge a health data access body is top-down. The designation of the respective bodies rests on the discretion of the Member State, and in the case where more than one body is designated, the Member State will recognise one of them as coordinator and contact point. As a result, bottom-up dynamics for data subjects' representation are curtailed.

Inextricably related to governance and the Health Data Access bodies are the provisions related to the infrastructural requirements of the EHDS. According to the proposal, access to, and processing of, health data will take place within a secure processing environment whose technical specifications (i.e. information security and interoperability) will be determined by the European Commission by means of implementing acts at a later stage.[24] However, this lack of prioritisation seems at odds with the reality of running data-intensive projects. This is because, in such cases, the technical requirements of the data infrastructure are at least equally significant to the legal norms that are supposed to regulate the transactions therein. Elbowing such issues aside can negatively affect the materialisation of the drafted legal principles. It also misdirects public dialogue by transforming important legal-political questions into technical challenges to be resolved by technical committees at a later stage. For this reason, there are important 'infrastructural' questions that need to be dealt in the 'here and now' of the legislative process. For instance, will the secure processing environment be supported by and operate within private cloud architectures? What will happen in those rare cases where access to health data is sought for an algorithmic project whose materialisation requires heavy computational capacity that cannot be supported by the native capabilities of the secure processing environment?

Finally, the Proposal introduces a cross-border infrastructure for secondary use of health data, the HealthData@EU, whose goal will be to facilitate health data exchanges among health data access bodies and authorised participants by adhering to the 'single application' principles according to which 'with one application, the data user obtains authorisation from multiple health data access bodies in different Member States'.[25] Contrary to EHR systems interoperability, there is some reference to privacy and data protection albeit in recital provisions:

> HealthData@EU should accelerate the secondary use of electronic health data while [. . .] respecting the privacy of natural persons and being interoperable. Due to the sensitivity of health data, principles such as 'privacy by design' and 'bring questions to data instead of moving data' should be respected whenever possible.

23. Open Future and Instrat, 'Feedback on the Proposal for a Regulation on the European Health Data Space' (23 July 2022), https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12663-Digital-health-data-and-services-the-European-health-data-space/F3327885_en
24. *Supra* note 2, Article 50 (4).
25. Ibid., Recital 57 & Article 45 (3).

However, apart from this declaratory principle that is to be followed 'whenever possible', the precise nature of the common specifications and the technical requirements underlying the HealthData@EU infrastructure are left to the discretion of the European Commission. There is no guidance as to how principles of privacy or data protection by design and by default will play out in the balance with interoperability.[26] In parallel, there is no certainty as to how this new call for interoperability will interplay with existing international data interoperability standards.[27]

## Moving forward

In principle, interoperability is a socio-technical and computational project worth pursuing by means of laws and/for standardisation. It can streamline administrative processes, facilitate evidence-based policy-making at a Union level, and unlock new opportunities and potentialities for research. At the same time, interoperability complicates the application and enforcement of data protection rights by pulling the citizen and her rights further apart. For large projects such as the EHDS to work, trust must be established; one way to achieve this is by demonstrating that the quest for efficiency in health research and administration does not entail privacy compromises. At the same time, the governance mechanisms in place need to be accompanied by a robust framework for accountability, transparency, and representation.

We recommend:

1. Adding explicit clauses for, or references to, the principles of 'data protection by design and by default', and 'privacy by design and by default' in the common specifications and relevant Annexes of the Proposal presaging the development of privacy-preserving protocols and standards for EHR interoperability;
2. Adding explicit clauses for user authentication and auditing of logs in the common specifications for EHRs and the relevant Annexes of the Proposal with reference to existing standardisation initiatives;
3. Explicitly acknowledging the importance of collaboration between the Market Surveillance Authorities provided for in Article 28 of the Proposal and the Directorate-General for Competition;
4. Creating stricter duties for data users based on the principles of altruism and the collective value of data. These duties should include putting in public domain inventions and discoveries resulting from the secondary use of health data or making data from their own private databases available for healthcare research;
5. Amending Article 36 to include provisions on the institutional structure of the Health Data Access Bodies, accompanied by measures for third-party representation therein; and
6. Incorporating the techno-legal discussion on the technical specifications of the secure processing environment, its modalities, and standards within the already established parliamentary discussion shared by LIBE and ENVI.

26. Ibid., Article 52 (13).
27. Horgan et al. (n 4), p. 1638.

## Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

## Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: For the first author, funding received from Fondation Botnar.

## ORCID iD

Petros Terzis https://orcid.org/0000-0001-8985-5651