
EUROPEAN JOURNAL OF HEALTH LAW 31 (2024) 497–517
European Journal of Health Law
BRILL | NIJHOFF
brill.com/ejhl

# Collaboration in Healthcare: Implications of Data Sharing for Secondary Use in the European Union

*Fanni Kertesz* | ORCID: 0009-0004-0692-8747
Faculty of Law, University of Groningen, Oude Boteringestraat 18,
9712 GH Groningen, The Netherlands
*kerteszfanni1996@gmail.com*

Received 12 September 2023 | Accepted 8 July 2024 |
Published online 22 August 2024

## Abstract

The European healthcare sector is transforming toward patient-centred and value-based healthcare delivery. The European Health Data Space (EHDS) Regulation aims to unlock the potential of health data by establishing a single market for its primary and secondary use. This paper examines the legal challenges associated with the secondary use of health data within the EHDS and offers recommendations for improvement. Key issues include the compatibility between the EHDS and the General Data Protection Regulation (GDPR), barriers to cross-border data sharing, and intellectual property concerns. Resolving these challenges is essential for realising the full potential of health data and advancing healthcare research and innovation within the EU.

## Keywords

European law – secondary use of health data and medical industry

## 1 Introduction

The healthcare sector is a rapidly expanding and developing industry that significantly impacts the world. In healthcare management, various transformations have taken place due to technological advancement in recent

Published with license by Koninklijke Brill BV | DOI:10.1163/15718093-BJA10133
© FANNI KERTESZ, 2024 | ISSN: 0929-0273 (print) 1571-8093 (online)
This is an open access article distributed under the terms of the CC BY 4.0 license.

times.[1] For example, a notable shift can be identified from a disease-centred to a patient-centred model as well as from a volume-based to a value-based healthcare delivery approach.[2] In modern healthcare systems understanding new diseases and predicting more accurate prognoses at earlier stages are inevitable.[3] Therefore, digitalisation can enhance strong and resilient health systems, ensure better healthcare and provide innovation in the European Union (EU)'s medical industry. In principle, the health sector in the European Union has a vast amount of data, but it lacks the capacity to utilise the benefits of such data for scientific purposes or to advance human well-being. Health data has the potential to enable the development of new medical products and treatments as well as to reshape and modernise the EU's healthcare systems.[4] To unlock the opportunities inherent in health data, the Commission has decided to publish the European Health Data Space (EHDS) Regulation Proposal, which seeks to create a single market for health data to enhance Europe's competitiveness. The EHDS Proposal has two aims: empowering people to have better control and use over their health data, which is called primary use, whereas secondary use entails that the generated health data is used for research, innovation, regulatory activities or policy-making purposes.[5]

The Proposal builds upon multiple pieces of EU legislation, although this paper is limited to the General Data Protection Regulation (GDPR). Special focus is given to the secondary use of health data in Chapter IV of the EHDS Proposal, as it represents a key factor in future research and development initiatives within the medical sector, thus playing a vital role in improving disease management and treatment outcomes. Neglecting the reuse of health data can have detrimental effects on the functioning of the EU health industry as

1 S.A. Senthilkumar, B.K. Rai, A.A. Meshram, A. Gunasekaran and S. Chandrakumarmangalam, 'Big Data in Healthcare Management: A Review of Literature', *American Journal of Theoretical and Applied Business* 4 (2018) 57–69; T. Huang and others, 'Promises and Challenges of Big Data Computing in Health Sciences', 2 *Big Data Research* 2 (2015) 2–11.

2 J. Cortada, D. Gordon and B. Lenihan, *The Value of Analytics in Healthcare* (IBM Global Business Services, Armonk, NY, 2012), available online at https://www.ibm.com/downloads/cas/NJA9K0DV (accessed 14 April 2023).

3 H. Asri, H. Mousannif, H. Al Moatassime and T. Noel, 'Big Data in Healthcare: Challenges and Opportunities', in *2015 International Conference on Cloud Technologies and Applications (CloudTech), Marrakech, Morocco, 2015*, pp. 1–7, doi: 10.1109/CloudTech.2015.7337020.

4 European Commission, *Communication from the Commission to the European Parliament and the Council, a European Health Dara Space: Harnessing the Power of Health Data for People, Patients and Innovation* (Communication) COM (2022) 196 final, 1.

5 S. Kohl, 'European Health Data Space Proposal Launched', *European Journal of Hospital Pharmacy* 29 (2022) 240.

it can undermine treating illnesses or the invention of new medical devices.[6] However, several legal obstacles related to data sharing for secondary use exist that should be highlighted.

## 2 Method

The primary focus will be on the impact of health data sharing on the EU healthcare sector. Challenges stemming from the interplay of GDPR and EHDS, in addition to the sharing and accessing of health data among Member States, along with intellectual and trade secret issues, could potentially have adverse effects not only on the entire EU market for innovative medical products and devices but also on EU citizens. Therefore, the research question aims to explore the impact of legal challenges associated with secondary health data sharing in Chapter IV of the EHDS on the establishment of a competitive health data market in the EU healthcare sector. Furthermore, this article will utilize the doctrinal legal research method to thoroughly examine and interpret primary and secondary law sources, such as Regulations, journal articles, and working papers. The primary focus will be on analysing documents from the European Commission and European Parliament. Additionally, it aims to propose effective solutions for addressing the legal implications.

Concerning legal issues within the EHDS, three notable challenges should be highlighted that pose a risk to the EHDS's primary goal of establishing a competitive health data market that fosters enhanced research and innovation in the EU. The first pertains to accessing and sharing secondary health data, as the GDPR creates several impediments to them. The second concerns health data sharing across Member States, and the third involves potential challenges related to intellectual property (IP) and trade secrets. As a result, the first chapter explores potential legal challenges between the EHDS and the GDPR, emphasising their adverse effects on accessing and reusing secondary health data between Member States. Differing rules relating to access to data for research purposes and limited data interoperability were among the few identified concerns.[7] In chapter two several barriers to cross-border health

6 A. Geissbuhler, 'Trustworthy Reuse of Health data: A transnational Perspective', *International Journal of Medical Informatics* 82(1) (2013) 1–9, 2–4.

7 M. Shabani, 'Will the European Health Data Space Change Data Sharing Rules?', *Science* 327(6587) (2022) 1357–1359.

data sharing are subject to analysis.[8] Lastly, the third chapter uses the pharmaceutical industry to exemplify potential consequences of IP and trade secret issues in the secondary use of health data within and outside the EU that can pose a threat to the functioning of the internal health data market. Each chapter provides recommendations and suggestions on how the EHDS can further be improved to achieve its intended objectives as outlined in the Proposal.

## 3 Tackling Data-Sharing Challenges Related to Secondary Use Posed by the EHDS as Proposed

This chapter delves into the legal obstacles related to sharing health data for secondary purposes. Specifically, Sections 3.1, 3.2 and 3.3 mainly examine the interplay between the EHDS and the GDPR surrounding the sharing of health data, whereas Section 3.4 provides amendments.

### 3.1 *Legal Issues with the Current EHDS Proposal as It Stands in Relation to the GDPR*

Recital 37 of the EHDS outlines the legal basis for the secondary use of health data in relation to Articles 9(2)(g), (h) (i) and (j) of the GDPR with respect to safe, lawful processing and access to electronic health data. Article 6 of the GDPR acts as another legal basis for the data applicant.[9] As the Proposal stands, it appears to have different legal issues and conflicts regarding the GDPR. Chapter IV of the Proposal outlines the criteria for the processing of secondary use of health data which poses risks to the rights of data subjects.[10] For example, Article 34 states the criteria for data access bodies when electronic health data can be processed. Article 34(1)(f) and (g) says that health data access bodies should give access to health data in those cases when the intended goal complies with purposes, such as development and innovation aimed at creating products or services that benefit public health, and social security. Another intention can be helping to test and evaluate algorithms such

8 R. Richards, 'Barriers on Cross-Border Sharing of Health Data for Secondary Use and Options to Overcome These', *European Journal of Public Health* 32(Suppl. 3) (2022) ckac129.367.

9 European Data Protection Board, *EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space* (12 July 2022), available online at https://edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202203_europeanhealthdataspace_en.pdf, para. 83 (accessed 20 April 2023).

10 *Ibid.*, paras 82 and 85.

as medical devices and AI systems.[11] The purposes for processing personal data to contribute to public health or social security are vague as it is not accurately delineated when there is a connection between them. For this reason, there is a risk of either the target initially foreseen by the Proposal not being fulfilled or the protection of personal data being violated as each Member State can use different grounds to justify the process of personal data. Article 34(1) of the EHDS includes multiple purposes for the secondary use of electronic health data, such as assisting public sector organisations or Union institutions and bodies to fulfil their tasks (Article 34(1)(b)) or education and teaching activities in health or care sectors (Article 34(1)(d)) which under the exceptions of processing special categories of personal data provided by Article 9(2) of the GDPR could be categorised on different grounds.[12] Article 9(2) allows the use of special categories of data, for instance, if the data subject gives explicit consent. Meanwhile, Article 6 outlines the lawfulness of processing, including when the processing is necessary to protect public interests or safeguard vital interests of the data subject.[13] The main issue with the criteria outlined in Article 34(1) is that Article 45 of the EHDS contains the conditions that data access applications shall fulfil for secondary use to get a data access permit (Article 46 of the EHDS).[14] Article 46 of the EHDS only focuses on the guidelines and principles embedded in the Proposal itself and does not provide clear guidance on how the data access permit is connected to the requirements of Articles 9(2) and 6 of the GDPR for the lawul processing of special categories of personal data. It is ambiguous when Article 9(2)(j) of the GDPR would apply, which allows the processing of personal data for purposes such as public interest, statistics, or scientific research in conformity with Article 89(1) of the GDPR.[15] Consequently, legally it is unclear how the data access permit provisions correspond with the GDPR, as Article 46 of the EHDS does not clearly state and specify how the data permit will be assessed and granted based on Article 9(2) of the GDPR.[16]

---

11 European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space* (Communication) COM (2022) 197 final, Article 34; *ibid.*, para. 87.

12 *Ibid.*

13 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1, Articles 6 and 9(2).

14 *Supra* note 11, Articles 45–46; *supra* note 9, para. 87.

15 *Supra* note 13, Article 9 (2)(j).

16 *Supra* note 9, para. 88.

### 3.2 *Legal Concerns for Data Sharing in the EHDS*

In addition, further legal uncertainties can be found under Articles 9(2) and 9(4) of the GDPR. Article 9(2) states the processing of special categories of personal data that can be conformed with Article 9(4) which says that Member States can retain or establish additional conditions, including restrictions, related to the processing of genetic data, biometric data, or health-related data.[17] The issue comes with the Proposal as it currently is imprecisely formulated and there is a lack of sufficient legal clarification on how Article 9(1) prohibits the processing of sensitive data, and how it will be protected considering the exceptions allowed by Articles 9(2) and 9(4).[18] As a result, it is not explicitly specified how the Proposal aims to reconcile with the existing national laws.[19] Further emphasis should be given to Article 33(5) of the Proposal, stating that if national law obliges the consent of an individual, health data access bodies should follow the provisions in Chapter IV of the EHDS to enable access to electronic health data. The consent required by the national law provision is not comprehensible and vague as it is not clear when the data access bodies are allowed to disregard the requirements laid down in national laws, especially when it falls under 9(4) of the GDPR that allows Member States to propose further standards and limitations in relation to health data.[20] Article 36 of the Proposal mentions the health data access bodies' tasks and responsibilities. Notably Article 36(2) sets forth that Member States should provide health data access bodies with technical, financial, and human resources, however, it is unclear whether these bodies need to have legal expertise as the cited article does not refer to it. As it was outlined under Article 46, health data access bodies are required to assess data applications and grant a data permit. In this regard, data access bodies must review the reasons for requesting access to health data and assess whether they meet the legal grounds, which necessitates legal knowledge and expertise that Article 36 is unclear about. The health data access bodies' assessment of the legal basis can be overturned and examined by the appropriate National Data Protection Authority (DPA).[21] The interplay and cooperation between the role of the health data access body and the

17 *Ibid.*; *supra* note 13, Article 9(2)(4).

18 *Supra* note 13, Article 9(1)(2)(4).

19 *Supra* note 9, para. 89.

20 *Ibid.*, para. 92.

21 European Commission, *What are Data Protection Authorities (DPAs)?*, available online at https://commission.europa.eu/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en (accessed 25 April 2023). DPAs are independent public authorities and are present in each Member State, whose main task is to investigate and supervise the data protection law. They handle complaints about violations of the GDPR.

DPA are not defined in the Proposal, causing legal uncertainties and confusion in terms of data protection issues, as it is ambiguous in which cases the DPA can overrule the national health data access bodies' assessments.[22]

### 3.3 *Further Possible Obstacles Concerning the GDPR and the EHDS*

The EHDS seeks to facilitate cross-border data sharing for secondary use by establishing national contact points where data users will be required to apply for data access permits. However, the EHDS does not provide sufficient explanation on which national law will be used for assessing the data application and granting data permits for cross-border health data sharing. In this case, the Proposal leaves the question open and unanswered whether the health data access bodies' laws from which the data applicant requires the health data will be applied to give data permits, or where the data applicant domiciles. There is also a lack of explanation and requirements on which legal basis will be examined by the health data access bodies for granting such permits. Moreover, Article 38(2) entails that health data access bodies are not obligated to disclose specific information to every individual about how their data is handled and used for projects that obtained data permits as otherwise Article 14 of the GDPR would require.[23] According to Article 14, if personal data has not been acquired from the data subject, the controller is obligated to supply the data subject with essential information, including the aim of the processing of personal data, the legal basis for processing, or the recipients of the personal data.[24] In contrast, data access bodies are only obliged to issue a general overview of the granted data permits in accordance with Article 46 of the EHDS. This exemption introduced by the EHDS might have unforeseen effects on the fundamental rights of data subjects since it is not clearly defined under which circumstances this exemption can be applied. There is a risk that people may not know for which purposes their personal health data will be used, which can pose a danger to the protection of natural persons regarding the processing of personal data that is a fundamental right under Article 8(1) of the Charter of Fundamental Rights of the European Union and under Article 16(1) TFEU which ensures every individual possessing the right to protection of their personal data.[25]

22 *Supra* note 9, para. 93.

23 *Ibid,* para. 94.

24 *Supra* note 13, Article 14.

25 *Supra* note 9, para. 95; *supra* note 13, rec. 1; Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C326/47, Articles 8(1) and 16(1).

### 3.4 *Key Considerations for Modifying the EHDS Proposal with Regards to the GDPR*

After presenting and highlighting the main potential data-sharing challenges in relation to the GDPR, it is necessary to propose amendments that the Commission should further consider. Regarding the vagueness of Articles 34 (1)(f) and (g), more focus should be on the wording of innovation and research purposes intended to benefit public health and social security as the connection between the two goals is not adequately described and unclear. Legal clarity is required in relation to the criteria for the process of secondary use of electronic health data under Article 34(1) and how it relates to the exceptions under Article 9(2)(j) of the GDPR.[26] Section 3.2 analyses the prohibition of special categories of data (Article 9(1) GDPR) and how the processing of sensitive data can be justified under Articles 9(2) and (4) of the GDPR.[27] Legal nuances are missing in the explanation of this matter and special focus should be made to indicate how the varying national laws will interact in the EHDS and will protect the interests of individuals. It can be argued that the different interpretations and differences between the legal grounds can further diminish the trust of citizens and possibly make cross-border data-sharing interactions more onerous. Regarding Article 36(2) of the EHDS, Member States should not only ensure that the data access bodies are equipped with human and capital resources but also have necessary legal expertise.[28] Therefore, arguably, the Commission should make amendments to include the phrase that Member States shall ensure that data access bodies have minimum legal expertise in order to properly assess the data access application pursuant to Articles 45 and 46 of the Proposal as cited under Article 37 of the EHDS. The interplay between the DPA and data access bodies should be better defined on how they will work and collaborate in respect of data protection.[29] Another interaction between the two legal frameworks calls for a need to underline when consent is required by national law for accessing electronic health data (Article 33(5) GDPR), the provisions of Chapter IV should be followed. However, it should be specified when each Member State is allowed to introduce further requirements for processing health data under Article 9(4) of the GDPR. As the two legal frameworks stand there is not enough insight on how the exceptions can be used and justified.[30] As anticipated, the Parliament proposed the inclusion

26 *Supra* note 9, paras 87–88.
27 *Ibid*, para. 89.
28 *Ibid*, para. 93.
29 *Ibid*.
30 *Ibid*, para. 92.

of an opt-out option, stating, "Natural persons shall have the right to opt-out of the processing of their electronic health data for secondary use," as per the amendment to Article 33.[31] Ensuring the option to opt-out of secondary use processing is essential to uphold the core principles of data protection rights (Article 9(2) GDPR). Moreover, this matter extends to the trust dynamic between patients and healthcare providers. Patients might be hesitant to share health data with healthcare providers if there's an automatic transfer of the data for secondary use without their consent. [32]This diverges from the Commission's proposal, which relied on the existing GDPR, known for its varying implementation across the EU. In the case of specific sensitive data categories, such as genetic and genomic information, MEPs took it a step further by introducing an explicit consent or opt-in system. This implies that every patient whose data falls under this category must provide consent each time the data is used. Health Commissioner Stella Kyriakides opposed the opt-out option, citing concerns about potential biases in the data. She argued that minority groups, if not adequately represented in the dataset due to opting out, could be negatively impacted, potentially hindering research and the development of new treatments or health applications that cater to their needs.[33] Further emphasis should be devoted to the exceptions provided by the GDPR and the EHDS concerning the potential loopholes that may arise in real scenarios and contexts. Even if consent is required by national law to process health data, and data access bodies follow the provisions in the EHDS, it is not explained what may happen if a Member State law has other requirements besides the consent by the data subject obligation. Section 3 analyses further legal problems between the EHDS and the GDPR, especially between Article 14 of the GDPR and Article 38(4) of the EHDS. They appear to conflict with respect to the information that data access bodies shall or shall not be obliged to provide to individuals.[34] Indeed, further specifications need to be given under

31 G. Peseckyte, 'EU Parliament agrees position on digitalizing health data', *Euractiv* (13 December 2023), available online at https://www.euractiv.com/section/health-consumers/news/eu-parliament-agrees-position-on-digitalising-health-data/ (accessed 15 January 2024).

32 European Parliament, *Draft Report on the proposal for a regulation of the European Parliament and of the Council on the European Health Data Space* (COM(2022)0197-C9-0167/2022-2022/0140(COD)) (10 February 2023), available online at https://www.europarl.europa.eu/doceo/document/CJ43-PR-742387_EN.pdf (accessed 15 January 2024).

33 *Ibid.*

34 *Supra* note 9, para. 95.

Article 38(4) as to why Article 14 of the GDPR is not applied in the case of the data access bodies and how it can enhance the protection of human rights.[35]

## 4 Barriers to Cross-Border Data Sharing of Secondary Use of Health Data

This section explores the barriers to health data sharing in the context of secondary use, including anonymisation, pseudonymization and interoperability concerns in Sections 4.1 and 4.2. Additionally, Section 4.3 investigates the complexities of sharing sensitive personal data, whereas Section 4.4 provides recommendations to address these issues.

### 4.1 *Legal Ambiguities as a Potential Hindrance to the Sharing of Health Data in the EU*

This section will explore several challenges related to the sharing of data across borders, especially the issues with anonymisation among Member States. Article 44 of the EHDS elaborates on the data minimisation and purpose limitation for granting access for the secondary use of electronic health data. Data access bodies are responsible for giving access to electronic health data in an anonymised way, only if the data access is in line with the goals stated in the data access application for which the data permit was given.[36] Recital 49 of the EHDS states that the privacy of natural persons shall be safeguarded and considering the sensitivity of electronic health data, the data minimisation principle should be applied as stated in Article 5(1)(c) of the GDPR. In other words, for the purpose of secondary use, health data should be anonymised. Such data shall be made available if it is feasible and the data user requests it.[37] Anonymisation is a process where it is indispensable to obscure or remove any personal information that can either disclose information about an individual or risk revealing their identities.[38] In terms of the obligations for anonymisation at national and international levels, scientists and policymakers highlighted the insufficient guidance on anonymisation as a potential obstacle to data sharing. Furthermore, data users claimed that the lack of a

35 Article 14 of the GDPR states that the data controller should provide the data subject with information if the data was not acquired from the data subject for the purposes of data processing.

36 *Supra* note 11, Article 44(1).

37 *Supra* note 11, rec. 49, *Supra* note 13, Article 5(1)(c).

38 R. Senigaglia, C. Irti and A. Bernes, *Privacy and Data Protection in Software Services* (Springer, Berlin, 2022), p. 52.

clear explanation of anonymisation processes causes uncertainty and halts cross-border data transfers since the various definitions of anonymisation within the Member State reduce the re-use of health data. One country can have stricter laws on anonymisation which can further impede the speed of innovation or outcomes of an investigation, study or inquiry.[39] Sometimes all data are treated as personal data under Article 9(1) of the GDPR which prohibits the processing of personal data in case it can reveal the identity of the individual.[40] As a consequence, it was also reported that over-anonymisation can reduce the reliability and quality of health data. Its usefulness in research can be diminished as conducting correlation studies sometimes demands connecting different pieces of individual data. However, the lack of connection between individual data points can result in difficulties in understanding and analysing their relationships.[41] In this sense, the EHDS may not achieve its objective to facilitate cross-border health data transfer or provide data access to public or private sectors to foster scientific progress.[42] Failing to comply with the data access bodies' rules respecting and protecting personal rights, implies appropriate fines (Article 44(3) EHDS).[43] In the event of a breach of the rights provided by the GDPR, data users and access bodies specified as joint controllers for data processing under the GDPR will be held liable for the damages.[44] It should be noted that the phrase 'appropriate penalties' is broad and does not specify whether these penalties should be subject to national laws, or EU laws. The absence of clear rules may lead to varying fines, which can be argued, may not effectively deter violating laws. Many scholars have emphasised differences in national legal systems regarding the violation of EU laws, and the different interpretations of appropriate penalties among Member States being problematic.[45] Applying the same arguments to the given example, another

39 L. Abboud, P. Bogaert, S. Bowers, H. Clissold, S. Cosgrove. I. Kesisoglou, R. Richards, C. Pinto, M. Saso and F. Soares, 'Report on Secondary Use of Health Data through European Case Studies', *Towards European Health Data Space* (28 February 2022), available online at https://tehdas.eu/app/uploads/2022/08/tehdas-report-on-secondary-use-of-health-data-through-european-case-studies-pdf, pp. 11–12 (accessed 10 April 2023).

40 *Supra* note 13, Article 9(1).

41 *Supra* note 39, p. 12.

42 *Supra* note 11, Article 5.

43 *Supra* note 11, Article 44(3).

44 D. Horgan, M. Hajduch, M. Vrana, J. Soderberg, N. Hughes, M.I. Omar, J.A. Lal, M. Kozaric, F. Cascini, V. Thaler, O. Solà-Morales, M. Romão, F. Destrebecq and E.S. Gross, 'European Health Data Space – An Opportunity Now to Grasp the Future of Data – Drives Healthcare', *Healthcare* 10 (2022) 1629.

45 European Commission, *Proposal for a Directive of the European Parliament and of the Council on the Definition of Criminal Offences and Penalties for the Violation of Union*

possible outcome can be divergent laws resulting in inconsistent penalties, which can entail a fragmented legal system within the EU and ultimately fail to protect the interests of the individuals. Indeed, it can lessen the citizen's trust and losing confidence in health data sharing can jeopardise the aims and objectives of the EHDS in relation to secondary use.[46]

### 4.2 *Pseudonymisation and Interoperability Issues: A Legal Challenge to the Success of Secondary Data Use*

If the intended data processing purpose is not achievable by having access to anonymised data, the health data access bodies should ensure access to pseudonymised data. Article 4(5) of the GDPR explains pseudonymisation as a process whereby personal data cannot be attributed to a data subject.[47] However, if public institutions, researchers, or companies are required to use personal electronic health data, the data access request should explicitly state the reasons why this type of data will be used. In those circumstances, access to personal electronic health data should be pseudonymised, i.e., data should provide information about the disease, medication, or symptoms, but the identity of the individual should be protected and cannot be revealed to the user. The health data access bodies can only have the encryption key for the data. Also, the data user is not allowed to re-identify the data subjects.[48] Furthermore, the controller must employ appropriate measures, such as pseudonymisation, to uphold data protection principles like data minimization. This ensures compliance with the GDPR and protects the rights of data subjects during both the determination of processing means and the processing itself.[49] Nevertheless, data users shed light on divergent interpretations with respect to pseudonymisation rules and standards as they cause interoperability issues across

*Restrictive Measures* (Communication) COM (2022) 684 final, 2. This resource demonstrates the legal challenges for the inconsistent interpretation of penalties and varying legal systems in the context of restrictive measure. F. Molnar-Gabor and others, 'Harmonization after the GDPR? Divergences in the Rules for Genetic and Health Data Sharing in Four Member States and Ways to Overcome them by EU Measures: Insights from Germany, Greece, Latvia and Sweden', *Seminars on Cancer Biology* 84 (2022) 271–283. This article emphasises the fragmented legal system in the EU when it comes to interpretation of law like the GDPR.

46 D. Horgan, B. Borisch, I. Cattaneo, M. Caulfield, A. Chiti, C. Chomienne, A. Cole, K. Facey, A. Hackshaw, M. Hendolin, N. Georges, D. Kalra, B. Tumienė and M. von Meyenn, 'Factors Affecting Citizen Trust and Public Engagement Relating to the Generation and Use of Real-World Evidence in Healthcare', *International Journal of Environmental Research and Public Health* 19 (2022) 1674.

47 *Supra* note 11, Article 4(5).

48 *Supra* note 11, Articles 10–11; *Supra* note 11, rec. 49.

49 *Supra* note 13, Article 25(1).

EU countries. The lack of consistency on when to use pseudonymised or anonymised data for health data sharing led to confusion and presented barriers to the interoperability of data.[50] The lack of consistent European interpretation of what can be considered secondary use of data showed another obstacle to health data sharing. The unanswered question of what constitutes secondary use raises challenges when consent is required for data sharing since it can be unclear to individuals what they have consented to when they have agreed to process their data.[51] If consent is compulsory for electronic data for secondary use under national law as it is outlined in Article 33(5) of the EHDS, and if patients do not give their consent, data processing may be hindered, hence undermining the development of new medicine to treat and cure serious diseases.[52] Even though the GDPR is a regulation meaning it is binding in its entirety and directly applicable, based on data users' reports, there are various interpretations of the GDPR across Member States.[53] It was reported that additional national rules on the secondary use of health data led to complications with respect to personal data sharing across the EU. In cases when there is a joint project across borders and cross-border health data processing is crucial, the GPDR allows Member States to set different derogations for scientific, statistical, or historical analysis purposes.[54] Various rules are used in how each State interprets the GDPR, as some countries tend to have stricter provisions than the GDPR, leading to a halt in cross-border scientific advancement and data sharing.[55]

### 4.3 *Personal Health Data: Special Treatment Mechanisms*

Data related to health is categorised as a special category of data within the framework of the GDPR. As such, it necessitates distinct approaches and management techniques compared to handling other types of data.[56] The GDPR sets strict rules for the processing of personal data which is prohibited according to Article 9(1) of the GDPR, however, derogations to the use of such data can be found under Article 9(2). Data users have indicated that the sensitive nature of health data can cause risk-averse behaviours, as data controllers tend to anonymise data to protect individuals' rights, resulting in reduced useability

50 *Supra* note 39, p. 13.
51 *Ibid.*, 14.
52 *Ibid.*; *supra* note 11, Article 33(5).
53 *Supra* note 25, Article 288. This article states 'a regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States.'
54 *Supra* note 13, Article 89.
55 *Supra* note 39, p. 17; A. Negrouk and D. Lacombe, 'Does GDPR Harm or Benefit Research Participants? An EORTC Point of View', *The Lancet Oncology* 19 (2018) 1278–1280, 1278–1279.
56 Health data is considered to be a special category of data under Article 9(1) of the GDPR.

and undermining the goals for secondary use laid down in the EHDS.[57] Data processing has further implications across the EU since data users also noted that the divergent legal basis for health data processing under the GDPR constitutes another hurdle. Articles 6 and 9 of the GDPR lay down the requirements for personal data processing and based on EU reports, European countries tend to use different legal basis for data processing.[58] It is important to mention that the lack of clarity on the legal basis for processing can cause data to be collected by using consent in one country, whereas in another state the same data is used on justifications as public interest. Such differences in the legal basis will also cause serious delays in scientific advancement and innovation as data controllers might have to apply distinct legal bases for the same processing. Article 89 of the GDPR provides derogations for the data subject rights which is dependent on the chosen legal basis. Due to the previously mentioned rights enacted in the GDPR, one controller may be obliged to use exemptions to particular rights in one country while a different controller may not apply the exemptions in another country or might apply only to a specific part of the data. Controllers who are obligated to carry out processing under consent, although the data was acquired by using a different legal basis, will be required to use the derogation provisions to lawfully handle and safeguard the rights and freedoms of the data subject.[59] The GDPR initially was designed to process personal data in all sectors across the EU and the aforementioned legal issues for research and innovation purposes were unintended.[60]

### 4.4 *Reforms Needed for Cross-Border Data Sharing*

Section 3 examines the EU standards on anonymisation in the GDPR and the EHDS and deducts that the current EU standards act as a barrier for cross-border electronic health data sharing and the re-use of health data in research.[61] To

57 *Supra* note 39, p. 20.

58 *Supra* note 13, Articles 6 and 9. Article 6 states the lawfulness of the processing of personal data. It can be legal if either the data subject has given consent, the processing is necessary for the performance of a contract, is in compliance with a legal obligation or the processing is necessary for the public interest. Another possible reason can be that the controller or a third party has a legitimate interest. Article 9 mentions that the processing of special categories of personal data is prohibited, however, under para. 2 there are some exceptions, such as the data subject has given explicit consent to the processing or it is necessary to protect the interests of the data subject.

59 *Supra* note 39, pp. 18–19; *ibid.*, Article 89.

60 D. Peloquin, M. DiMaio, B. Bierer and M. Barnes, 'Disruptive and avoidable: GDPR Challenges to Secondary Research Uses of Data', *European Journal of Human Genetics* 28 (2020) 697–705.

61 *Supra* note 39, pp. 11–12.

solve the problem, the Commission should amend the data minimisation and purpose limitation article (Article 44 EHDS) to specify the possible legal basis for anonymisation how it can be achieved and which exceptions can apply. An additional solution can include a definition of anonymisation under Article 2 of the EHDS to provide an accurate meaning, and to avoid the obstacles with data sharing and interpretations. Section 3.1 elaborates on the issues related to the violation of the protection of individual rights and not complying with the data access bodies' measures with anonymisation. Such violations shall imply appropriate penalties (Article 44(3) EHDS).[62] Arguably, the phrase 'appropriate penalties' should be mandated to be transparent and provide an accurate explanation halting the possibilities of inconsistent fines and the lack of protection of rights and freedoms. Section 3.3 shows that anonymisation and pseudonymisation are not the only problems with electronic health data sharing when it comes to data interoperability, but the interpretation of secondary use.[63] While Article 2(2)(e) only provides a definition of what constitutes secondary use enacted in the EHDS, Article 35 sets the criteria for the prohibition of secondary use of electronic health data, but as the evidence shows, the given criteria are not enough and will cause implications in the legal sphere. For that reason, Article 35 should be amended or Article 2(2)(e) should include a more precise interpretation of the secondary use. Section 3.3 mentions that the legal basis among Member States varies, thus data can be processed on different grounds, which can hamper scientific research and innovation. Either Article 6 or 9 of the GDPR can be used to process data, however, the EHDS shall consider the potential consequences of this legal issue to make the data transfer more attractive in connection with research institutions or private companies. Further emphasis should be placed on the secondary health data sharing between the EU and third countries, as the current proposal in Article 52(5) and in the explanatory memorandum lacks justifications on why the EU should share health data outside the European Economic Zone.[64] Consequently, possible amendments should be considered to better understand how the EU's aim of establishing a healthy union and improving the internal market, while promoting research and innovation will align with the purposes of providing health data to third countries.[65]

62 *Supra* note 11, Article 44.
63 *Supra* note 39, pp. 13–14.
64 *Supra* note 11, Article 52(5).
65 *Supra* note 11, p. 5.

## 5 The EHDS's Impact on the Pharmaceutical Industry

This section examines the consequences of the EHDS on the whole EU medical sector, particularly by negatively influencing research and development (R&D), with the pharmaceutical industry serving as a prime example. IP and trade secrets are integral components of the secondary use of health data, serving as essential resources to support and supply research and innovation purposes in the EHDS. Therefore, it is important to analyse their legal effects on pharmaceutical companies since the lack of sufficiently defined legal remedies and protection can risk the objectives of the EHDS. It is important to acknowledge that the analysis should consider a wider context, the transfer and exchange of health care data not only between Member States but between the EU and third countries. For this reason, Section 5.1 introduces the ramifications of legal issues around the GDPR and the EHDS on the pharmaceutical industry in and outside the EU. In Section 5.2 attention is given to the intellectual property (IP) and trade secret issues that exist in the EHDS and the possible effects they can have on the pharmaceutical market.[66] Section 5.3 emphasises the consequences of IP and Trade Secret Protection and Section 5.4 explores possible solutions to these challenges.

### 5.1 *Global Implications of the EHDS: Examining Challenges in International Health Data Exchange*

The EHDS does not emphasise the need to establish a global data exchange system. Article 52 of the EHDS states that third countries or international organisations may become authorised participants in case they comply with the rule in Chapter IV of the Regulation, whereas the preamble only states that it was established to improve the functioning of the internal market, thereby deterring scientific research and development initiatives and decreasing investment in the EU industry.[67] Conversely, the Proposal does not explicitly state whether third countries would reciprocate by sharing health data with the EU, raising questions about the potential benefits to the EU's pharmaceutical industry and why such data sharing is advantageous for the EU. The restricted access to personal health data from the EU to third countries can influence the global sharing of data for research and development initiatives. The abovementioned

66 *Supra* note 11, p. 4.

67 Bio.News, 'How the European Health Data Space (EHDS) Will Impact Companies Operating in the EU', *Bio.News* (22 September 2022), available online at https://bio.news/international/how-the-european-health-data-space-ehds-will-impact-companies-operating-in-the-eu/ (accessed 18 April 2023).

issues with the relationship between the EHDS and the GDPR, examined in Chapters 1 and 2, explain how the interactions between the legal frameworks impede the secondary use of personal electronic health data within the EU. When it comes to sharing personal health data with reference to Article 9 of the GDPR, without proper compliance with the criteria, it is deemed unlawful. Under the EHDS, it is the responsibility of each Member State to assess whether the intended purposes comply with GDPR Regulation. This results in fragmented legal systems within the EU, marked by varying interpretations and implementation methods. Without dealing with the issue, the GDPR could impede the sharing and processing of secondary use of health data within and outside the EU, to the detriment of related pharmaceutical companies. Due to the unclear measures regarding the global transfers of health data for research and innovation in the EU (Article 52(5) EHDS), small and medium-sized companies and researchers may also be affected. The legal uncertainties around the restrictions of data transfer and fractured legal systems may not strengthen but rather harm biotech companies and affect early R&D efforts.[68]

### 5.2 *The Devil is Always in the Detail* (*Legal Issues about IP and Trade Secrets*)

Under Article 2(2)(y) of the Proposal data holders are defined as individuals or organisations including those in the health or care sector, conducting research in connection with the earlier-mentioned sectors, bodies, offices, agencies or Union institutions who have the ability to provide specific data. Based on Article 2(2)(y), pharmaceutical companies can be considered as data holders in the sense of the EHDS. The Proposal builds upon safe electronic health data systems where data can be accessed and processed securely. Until recently, no further explanation was provided on how safe processing environments will work with respect to IP and trade secrets.[69] There are various concerns regarding the proposed EHDS, as it can undermine the rights of intellectual property and trade secrets holders.[70] Article 33(4) states that electronic health data involving IP and trade secrets from private companies should be provided for

68 *Ibid.*; *supra* note 11, Article 52(5).

69 A. McFadyen, 'What the European Health Data Space Means for Pharmaceutical Companies', *Pinsent Masons* (30 September 2022), available online at https://www.pinsentmasons.com/out-law/analysis/european-health-data-pharmaceutical-companies (accessed 26 April 2023).

70 MedTech Europe, 'MedTech Europe's Position on the Proposed European Health Data Space Regulation', *MedTech Europe* (2023), available online at https://www.medtecheurope.org/wp-content/uploads/2023/02/230222-ehds-position-paper-final.pdf, p. 12 (accessed 28 April 2023).

secondary use and in such cases, appropriate safeguards should be considered to ensure confidentiality. Also, Recital 40 of the EHDS makes it compulsory to disclose data that benefits pharmaceutical companies or medical device companies in order to protect human health.[71] The Proposal makes it obligatory for data holders to share their electronic health data with other data users for the purposes of secondary use.[72] Moreover, the EHDS is uncertain and imprecise about the safeguards in place and the adequacy and enforceability of the measures to protect IP and trade secrets. This legal vagueness appears to weaken the rights of IP owners and trade secret holders who have devoted a substantial number of resources to gather data, hence private companies can be less motivated to take risks and invest in new innovations, which would be contrary to the EHDS' vision.[73] EU and national laws provide protection for IP and trade secrets and sufficiently regulate the interests of individuals. Any infringement upon such rights should entail a proportionality assessment. In other words, the interference should be evaluated based on legal grounds to validate whether it can be justified. Nevertheless, the EHDS as it stands, does not include the proportionality assessment on the cited rights.[74] Under Recital 40 it only mentions that in certain circumstances, such as a pandemic or public health crisis, the IP data should be made accessible to public authorities or regulators. In this sense, the EHDS states 'justifications' for the interference of such rights, however, it does not solve the question of how and when these rights can be further protected.

### 5.3 *Consequences of Inadequate IP and Trade Secret Protection*

The European Union has the second-largest pharmaceutical market in the world, involving a broad spectrum of stakeholders, like start-ups and producers of patented medicines or generics.[75] One of the main risks that the current provisions can cause to manufacturers of medical technologies or pharmaceutical companies is the chance that the invested efforts and money in new technologies will not be recouped, or will not create an advantage in the competition, to

71 *Supra* note 11, Article 33(4) and rec. 40.

72 *Supra* note 71, p. 12.

73 Digital Europe, 'DIGITALEUROPE's Position Paper on the European Health Data Space Proposal', *Digital Europe* (19 January 2023), available online at https://digital-europe-website-v1.s3.fr-par.scw.cloud/uploads/2023/01/DIGITALEUROPEs-Position-Paper-on-the-European-Health-Data-Space-proposal-1.pdf (accessed 21 April 2023).

74 *Supra* note 71, p. 12.

75 European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Pharmaceutical Strategy for Europe* COM (2020) 761 final, 2.

the detriment of the companies. As a result, this could discourage innovation in the EU as well as on a global scale. Another detrimental consequence can be court litigation with IP and trade secret rights, as each Member State has divergent standards and national courts tend to rule differently. In the context of data requests, there is a possibility that competitors in the pharmaceutical sector will need access to data and it is uncertain who will be responsible for assessing the violation of IP and trade secret rights and whether adequate measures will be taken for providing protection. Such legal clarity and protection of existing rights are crucial to help establish an appealing market for the pharmaceutical industry to deliver innovation and provide new advanced technologies for EU citizens.[76] Granting intellectual property rights is not only inevitable, as it incentivises pharmaceutical companies to engage in R&D, creating economic growth, and increasing competition within the EU. Companies must innovate to be able to compete on performance, and intellectual property rights can be seen as a catalyst of undistorted competition.[77] The Pharmaceutical Strategy for Europe is one of the works that the EHDS with health data access tries to support.[78] The Pharmaceutical Strategy for Europe has significant importance in supporting innovation and competitiveness in the EU pharmaceutical industry. Furthermore, it will ensure that patients can get not only innovative but affordable medicines.[79] There is a potential risk that the above-mentioned issues regarding IP and trade secrets will hinder the effectiveness of the EHDS and will not achieve its intended purpose of supporting the work of the Pharmaceutical Strategy for Europe.[80]

### 5.4 *Importance of IP and Trade Secret Amendments*

The fact that private companies should give access to IP and trade secrets in relation to health data seems to undermine the previously stated objectives of the EHDS.[81] Therefore, the Proposal should amend Article 33(4) in a way to include the remedies in case of the violation of the rights and include a proportionality assessment to check whether the infringements of the rights

76 *Supra* note 71, p. 12.

77 O. Gurgula, Strategic Patenting by Pharmaceutical Companies- Should Competition Law Intervene?', *International Review of Intellectual Property and Competition Law* 51 (2020) 1062–1085, 1070.

78 *Supra* note 11, p. 4.

79 *Ibid.*; *supra* note 75. The Pharmaceutical Strategy for Europe states that good health is key to wellbeing that relies on various factors such as healthy lifestyle or fair and equal access to healthcare services.

80 *Supra* note 11, p. 4.

81 *Ibid.*, Article 33(4).

can be justified. The amendment should include and refer to the Trade Secrets Directive to protect trade secrets and IP rights.[82] On December 20, 2023, the European Parliament took a significant step in the EHDS legislative process by adopting its stance and initiating subsequent discussions with Member States to finalise the legislation. The EP with the new initiative on the EHDS Proposal has modified Article 33(4) of the EHDS by removing it and incorporating a provision stating that health data access bodies must safeguard the confidentiality of data, ensuring that such rights are not violated. Additionally, the health data access body is required to deny access to data if the measures specified in point 33 (a) are insufficient to protect intellectual property rights, maintain the confidentiality of trade secrets, or safeguard data protected by regulatory data protection for regulatory approval.[83] The recently introduced amendments affirm the legitimacy of the previously examined legal concerns, indicating a potential risk that the EHDS Proposal for the secondary use of health data may not effectively establish a competitive market.

## 6 Conclusion

The healthcare sector is undergoing rapid and dynamic changes, necessitating a transformative shift towards digitalisation to advance and improve health systems within the European Union's medical industry. This evolution is driven by the growing need for better approaches to disease diagnosis and treatment. The integration of digital technologies is becoming increasingly imperative to ensure better healthcare outcomes and foster innovation, addressing the evolving challenges and demands of the modern healthcare systems in the EU.[84] Recognizing this imperative, the Commission, through the EHDS, envisions the establishment of an appealing and competitive health data market in the EU, facilitating data sharing across Member States.

However, the Proposal, with its dual aim of granting individuals better access and control over their health data (primary use) while leveraging generated health data for research, regulatory activities, or innovation (secondary use), is confronted by multiple legal complexities.[85]

82 *Supra* note 74; *Supra* note 71, p. 12.

83 European Parliament, *Amendments adopted by the European Parliament on 13 December 2023 on the proposal for a regulation of the European Parliament and of the Council on the European Health Data Space* COM(2022)0197-C9-0167/2022-2022/0140(COD), amendments 310 and 315.

84 *Supra* note 1, 57; *Supra* note 4, 1.

85 *Supra* note 5, 40.

Chapter one sheds light on the interplay with the GDPR, revealing adverse effects on accessing and reusing secondary health data between Member States. Chapter two analyses barriers to cross-border health data sharing, hindering the EHDS's goal of establishing a health data infrastructure in Europe. The third chapter uses the pharmaceutical sector to illustrate the possible outcomes of intellectual property (IP) and trade secret challenges in the secondary use of health data both within and beyond the European Union. Special attention should be devoted to the legal issues about the IP and trade secrets in the EHDS, as there is a lack of clarification on how they are protected, and under which grounds the interference of these rights can be justified.[86] After analysing and examining the legal problems throughout the three chapters, it can be concluded that the EHDS lacks clarifications in different matters. Therefore, given the contested examples, it can be argued that as the current Proposal stands it will not benefit the EU internal health data market. This shortfall could potentially lead to outcomes contrary to the envisioned objective, emphasising the need for comprehensive and precise legal frameworks to navigate the complexities of health data sharing and access within the European healthcare sector.[87]

**Acknowledgements**

I would like to express my sincere gratitude to my supervisor, Dr. Jacquelyn Veraldi for her unwavering support and invaluable inspiration throughout this journey. I am also sincerely thankful to Dr. Richard Rak for his belief in my work and for sharing insightful ideas that greatly contributed to this article.

86 *Supra* note 93.
87 *Supra* note 5, 40.