Online First

ISSN 2281-5147

THE STRANGE CASE OF HEALTH DATA SHARING: TRADE SECRETS AND THE EUROPEAN HEALTH DATA SPACE

Paolo Guarda*

Abstract

This article examines the role of trade secrets within the European Health Data Space Regulation (EHDS), focusing on the tension between the secondary use of electronic health data and the protection of commercially valuable information. The EHDS is the first major sector-specific test of the European Data Strategy in the health sector. It promises to make health data available for research, innovation, policy-making, regulatory activities and the development and evaluation of AI systems. Yet this promise depends on the capacity of the legal framework to manage interests that do not naturally point in the same direction.

The article argues that Article 52 EHDS is the key provision for governing this conflict. It does not treat intellectual property rights, trade secrets or regulatory data protection as automatic vetoes against access. Rather, it requires protected electronic health data to be made available for secondary use while entrusting Health Data Access Bodies with the task of adopting specific, appropriate and proportionate preservation measures. In this sense, Article 52 proceduralises the conflict between openness and secrecy.

The article identifies three implementation risks: overclaiming by data holders, uneven institutional expertise and fragmentation across Member States. It then situates the EHDS within the broader EU data law framework and uses legal interoperability, comparative approach and interdisciplinarity as tools for moving from regulatory narratives to operational governance. The article concludes that the success of the EHDS will depend on making secrecy governable without allowing secrecy to govern the data space.

* Associate Professor of Comparative Private Law, Faculty of Law - University of Trento. This paper was presented at the 2026 LawTech Consortium, Faculty of Law - The University of Hong Kong, Hong Kong, May 29-30, 2026, paolo.guarda@unitn.it

Online First

ISSN 2281-5147

Table of Contents

Keywords

European Health Data Space - Trade secrets - Secondary use of health data - Article 52 EHDS - Legal interoperability - Health Data Access Bodies - Regulatory fog

1. Introduction: health data between openness and secrecy

Collaboration and knowledge sharing are essential in the medical and biomedical fields. Scientific progress depends on the possibility of accessing reliable evidence, testing hypotheses on sufficiently rich datasets, comparing results and reusing data under trustworthy conditions. The COVID-19 pandemic confirmed the importance

Online First

ISSN 2281-5147

of open science and rapid data exchange, while also revealing how difficult it remains to balance openness with privacy, intellectual property, confidentiality and other legally protected interests[1].

The European Union has responded to these tensions through a broader regulatory project named "European Data Strategy". The declared objective is to create a single market for data in which information can circulate across sectors and Member States for the benefit of businesses, researchers, public administrations and society at large[2]. The strategy includes several legislative instruments: the Open Data Directive, the Data Governance Act, the Data Act, the Artificial Intelligence Act, the Digital Services Act and the Digital Markets Act [3]. These instruments must also be coordinated with the General Data Protection Regulation (GDPR), intellectual property laws, competition law, contract law and sector-specific health regulations.

---

[1] Paolo Guarda, Giorgia Bincoletto, 'Scientific Research and the Biomedical Sector. Requirements and Methods for Planning and Managing a Data Protection by Design Project' in Valentina Colcelli, Roberto Cippitani, Cristoph Brochhausen-Delius and Rainer Arnold (eds), *GDPR Requirements for Biobanking Activities Across Europe* (Springer 2023) 371; Rossana Ducato, 'Data Protection, Scientific Research and the Role of Information"(2020) 37 Computer Law and Security Review 105412; Lonni Besançon et al., 'Open Science Saves Lives: Lessons from the COVID-19 Pandemic' (2020) bioRxiv https://doi.org/10.1101/2020.08.13.249847; Roberto Caso, *La rivoluzione incompiuta. La scienza aperta tra diritto d'autore e proprietà intellettuale* (Ledizioni 2020).

[2] European Commission, A European Strategy for Data (Communication) COM(2020) 66 final; Giorgio Resta, 'Pubblico, privato, collettivo nel sistema europeo di governo dei dati' (2022) 4 Rivista trimestrale di diritto pubblico 971.

[3] Directive (EU) 2019/1024 on open data and the reuse of public sector information [2019] OJ L 172/56 (Open Data Directive-ODD); Regulation (EU) 2022/868 on European data governance [2022] OJ L 152/1 (Data Governance Act- DGA); Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data [2023] OJ L 2023/2854 (Data Act-DA); Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence [2024] OJ L 2024/1689 (AI Act); Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L 277/1; Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L 265/1.

ISSN 2281-5147

The European Health Data Space Regulation (EHDS) is the first major sector-specific test of this strategy[4]. It establishes an ecosystem composed of rules, standards, infrastructures and governance mechanisms for the primary and secondary use of electronic health data. Its objectives are twofold, since it aims to: empower individuals by improving access to and control over their personal electronic health data, including across borders; and enable the reuse of health data for purposes such as scientific research, innovation, policy-making, health threats preparedness, patient safety, personalised medicine, official statistics and regulatory activities[5].

This latter dimension is particularly important for data-driven medicine. Secondary use of health data may support epidemiological research, the evaluation of medical devices and medicinal products, the development and validation of artificial intelligence systems, and the design of public health policies. However, it also brings to the surface a structural conflict. The same datasets that are valuable for research and public health may also contain commercially valuable information, confidential know-how, curated database structures, processing pipelines, labelling strategies or proprietary analytical methods. In some cases, these elements may be protected as trade secrets.

Trade secrets are therefore a hidden antagonist in the EHDS story. They are not the protagonist of the Regulation, whose narrative is dominated by access, reuse and interoperability. Yet secrecy may redirect the plot. A legal regime designed to protect confidential business information against unlawful acquisition, use or disclosure may become, in the data economy, a strategic argument to resist access duties and transparency claims. This functional shift is particularly problematic where data sharing is justified by public interest, scientific research or health policy.

The central research question of this article is therefore whether trade secrets operate as an enabler or a disabler of an interoperable European digital healthcare system.

[4] Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 [2025] OJ L 2025/327.

[5] Regulation (EU) 2025/327, rec 1 and art 53. On secondary use of health data under the EHDS and its connection with the GDPR and AI systems, see Irene Sanchez Frias, 'Secondary Uses of Health Data under the European Health Data Space. Connections with the GDPR and the Impact of AI' (2025) 65 Revista General de Derecho Europeo 212.

ISSN 2281-5147

The answer cannot be binary. Trade secret protection may support innovation by preserving incentives for private and public actors that invest in data collection, curation and analysis. At the same time, excessive reliance on secrecy may undermine the very objectives of the EHDS, especially when it is used to restrict access to datasets otherwise covered by secondary-use obligations.

The article proceeds as follows. Section 2 reconstructs the EHDS as an access-governance infrastructure rather than a centralised database. Section 3 discusses the essential features of trade secret protection and its role in the data economy. Section 4 analyses Article 52 EHDS and argues that it proceduralises the conflict between openness and secrecy. Section 5 identifies three implementation risks: overclaiming, institutional expertise and fragmentation. Section 6 connects the EHDS with the broader European data law framework, including the Data Governance Act and the Data Act. Section 7 brings together legal interoperability, a comparative approach and interdisciplinarity as analytical tools for moving from regulatory narratives to operational governance. The conclusion returns to the Jekyll-and-Hyde metaphor and suggests that the future of the EHDS will depend on the ability to transform the promise of health-data sharing into workable access conditions.

2. The EHDS as an access-governance infrastructure for health data

Rather than establishing a central European archive of health data, the EHDS sets up an access-governance infrastructure: a framework of roles, procedures, technical standards, governance mechanisms and safeguards designed to make health data available under controlled conditions[6].

As regards primary use, the EHDS focuses on electronic health data processed in the context of healthcare provision. It is designed to improve continuity of care, cross-border healthcare services and individual access to electronic health records. It interacts with national systems of electronic health records, which remain diverse in

[6] Regulation (EU) 2025/327, recs 1 and 52. On obstacles in the creation of the EHDS, see Anastasiya Kiseleva, Paul De Hert, 'Creating a European Health Data Space: Obstacles in Four Key Legal Areas' (2021) 5 European Pharmaceutical Law Review 21.

ISSN 2281-5147

terms of technical design, governance and legal implementation[7]. This national diversity makes interoperability a practical and legal challenge.

For secondary use, the EHDS establishes a controlled access mechanism. Article 51 identifies minimum categories of electronic health data that shall be made available for secondary use. Data users must submit applications to Health Data Access Bodies (HDABs), which are entrusted with the assessment of the application and the issuing of data permits[8]. Access should normally be granted to anonymised data. Access to personal electronic health data may be authorised only where the applicant demonstrates that the intended purpose cannot be achieved with anonymised data[9].

The Regulation entered into force on 26 March 2025, but its application is staggered. Article 105 operates as the temporal coordination provision of the EHDS: it determines when the different parts of the Regulation become applicable, without altering the substantive scope of the data categories listed in Article 51. For the purposes of secondary use, Chapter IV applies from 26 March 2029. However, the availability of some categories of electronic health data is deferred: Article 51(1)(b), (f), (g), (m) and (p) applies from 26 March 2031. Participation by third countries and international organisations under Article 75(5) is further postponed until 26 March 2035. The transitional architecture is therefore significant not because Article 105 defines the relevant data, but because it determines the temporal sequence through which the EHDS will become operational.

This transitional dimension is important for the present analysis. The EHDS is no longer merely a legislative proposal, but it is not yet a fully operational infrastructure. It is an adopted framework whose effects will depend on implementation. This makes the rules on trade secrets particularly significant. If they are applied in an excessively restrictive manner, they may reduce the availability of data for secondary use. If they

[7] In Italy, for example, the "Fascicolo Sanitario Elettronico" has undergone significant reform and is now referred to "FSE 2.0". See Decree of the Italian Ministry of Health of 7 September 2023, implementing art 12(7) of Decree-Law No 179/2012; Giorgia Bincoletto, *Data Protection by Design in the E-Health Care Sector: Theoretical and Applied Perspectives* (Nomos 2021) 229-83.

[8] Regulation (EU) 2025/327, arts 51, 67 and 68.

[9] Regulation (EU) 2025/327, art 68.

ISSN 2281-5147

are applied in an excessively permissive manner, they may weaken legitimate interests of data holders and reduce incentives to invest in data-related innovation.

The EHDS is thus built on a promise: moving from locked data to shared knowledge. Health data can support open science, data-driven medicine, clinical insight and AI development only if access conditions are sufficiently clear and trustworthy. The problem is that the same data ecosystem also contains forms of control, commercial value and strategic secrecy. The Regulation must therefore manage a duality: openness as a public-interest objective and secrecy as a legally recognised interest.

3. Trade secrets in the data economy

Trade secrets are regulated in the European Union by Directive (EU) 2016/943 on the protection of undisclosed know-how and business information against unlawful acquisition, use and disclosure[10]. The Directive harmonised essential aspects of trade secret protection across Member States and introduced a common definition. Under Article 2(1) information qualifies as a trade secret where it is secret, has commercial value because it is secret, and has been subject to reasonable steps, under the circumstances, to keep it secret.

Trade secret protection is different from traditional intellectual property rights. It does not require registration. It may last indefinitely, as long as the information remains secret and the other requirements are satisfied. It does not confer ownership over data as such, but it operates as a form of "quasi-exclusivity" over information. It allows the holder to react against unlawful acquisition, use or disclosure, while leaving lawful means of acquisition, such as independent discovery or reverse engineering, outside the scope of liability[11].

[10] Directive (EU) 2016/943 on the protection of undisclosed know-how and business information against unlawful acquisition, use and disclosure [2016] OJ L157/1. See Davide Arcidiacono, 'The Trade Secrets Directive in the International Legal Framework' (2016) 1 European Papers 1073; Valeria Falce, 'Tecniche di protezione delle informazioni riservate - Dagli accordi TRIPS alla direttiva sul segreto industriale' (2016) Rivista di diritto industriale I 129.

[11] Directive (EU) 2016/943, arts 3-4. On the nature of trade secret protection, see Luigi Carlo Ubertazzi (ed), *Commentario breve alle leggi su proprietà intellettuale e concorrenza* (7th edn, CEDAM 2019)

ISSN 2281-5147

The rationale of trade secret law is usually connected with innovation, investment and fair competition. Firms may need to protect confidential know-how, research results, business strategies, technical processes or commercial information. In sectors where patent protection is unavailable, unsuitable or strategically undesirable, secrecy may become particularly attractive. In biomedical research, trade secrets may concern pharmaceutical information, clinical trial data, protocols, data curation practices, research pipelines, analytical tools and other forms of confidential knowledge.

The Directive was not enacted specifically for the data economy. It is a technologically neutral regime covering a broad range of know-how and business information[12]. Nevertheless, it has become increasingly important for data-driven activities. In a data-centric environment, commercial value may reside not only in individual items of information, but also in the organisation, selection, curation, labelling, structuring, enrichment and processing of datasets. A single health datum will rarely have standalone commercial value because it is secret. Aggregated datasets, curated databases, data processing pipelines and proprietary algorithms are more likely to satisfy the commercial value requirement[13].

This point is crucial for the EHDS. The Regulation concerns electronic health data and datasets that may be generated, collected or held by a variety of actors, including public bodies, healthcare providers, research institutions and private companies. Some of these actors may claim that the data requested for secondary use contain information protected by trade secrets or intellectual property rights. Such claims may refer not only to the content of the data, but also to the way in which the dataset has been structured, cleaned, annotated or combined.

608-10; Estelle Derclaye, Matthias Leitner, *Intellectual Property Overlaps: A European Perspective* (Hart 2011) 21 ff, 172 ff, 223 ff.

[12] Directive (EU) 2016/943, rec 2; Tanya Aplin, Alfred Radauer, Martin A. Bader and Nicola Searle, 'The Role of EU Trade Secrets Law in the Data Economy: An Empirical Analysis' (2023) 54 IIC 826; Ana Nordberg, 'Trade Secrets, Big Data and Artificial Intelligence' in Jens Schovsbo, Timo Minssen, Thomas Riis (eds), *The Harmonization and Protection of Trade Secrets in the EU: An Appraisal of the EU Directive* (Edward Elgar 2020) 194; Josef Drexl, *Data Access and Control in the Era of Connected Devices* (BEUC 2018).

[13] On trade secrets and datasets in the data economy, see Aplin, Radauer, Bader and Searle (n .12) 841-44.

ISSN 2281-5147

The strategic role of trade secrets has therefore shifted in a problematic direction: from a defensive mechanism against unlawful acquisition, use or disclosure to a possible instrument for resisting access obligations, transparency requests or data-sharing duties. Trade secrets may thus become a legal device through which duties of data openness are limited, delayed or reshaped.

The EU legislature was aware of the need to balance secrecy and the public interest. Recital 21 of the Trade Secrets Directive states that measures, procedures and remedies should not undermine fundamental rights and freedoms or the public interest, including public health. Article 5 also provides exceptions, including where disclosure serves the public interest in revealing misconduct, wrongdoing or illegal activity. These provisions show that trade secrets are not absolute. Article 52 EHDS develops this logic in the specific context of secondary use of electronic health data.

4. Article 52 EHDS: proceduralising the conflict

Article 52 EHDS is the key provision governing the relationship between electronic health data, intellectual property rights, trade secrets and regulatory data protection. Paragraph 1 establishes the starting point: electronic health data protected by such interests shall nevertheless be made available for secondary use in accordance with the Regulation. The provision therefore rejects the idea that the mere existence, or allegation, of trade secret protection can operate as an automatic veto against access.

Paragraph 2, then, introduces a disclosure and justification duty for health data holders. Where the data include information protected by intellectual property rights, trade secrets or regulatory data protection, the holder must inform the relevant HDAB, identify the data concerned and justify the need for specific protection. This is a crucial step because trade-secret protection is not subject to registration or prior administrative validation. The legal status of the asserted secret must therefore be made visible and reviewable within the access procedure, otherwise the risk of generic or defensive claims would be particularly high[14].

[14] On the absence of ex ante confirmation of trade-secret qualification and the risk of overclaiming in data access settings, see Ulla-Maija Mylly, 'Trade Secrets and the Data Act' (2024) 55 IIC 368.

ISSN 2281-5147

Paragraph 3 shifts the analysis from the existence of protected interests to their preservation. The HDAB must take specific, appropriate and proportionate measures to preserve intellectual property rights, trade secrets and regulatory data protection while enabling access to the extent possible. These measures may be legal, organisational or technical in nature. They may include confidentiality duties, access restrictions, secure processing environments, limitations on copying or downloading, logging and audit mechanisms, output checking, or other safeguards capable of reducing the risk that the protected information is disclosed or used beyond the authorised purpose.

Paragraph 4 adds a conditional-access layer. The HDAB may make access to electronic health data subject to the implementation of preservation measures by the health data user. Contractual arrangements may therefore become an important instrument for translating the general duty to preserve secrecy into concrete obligations. The Regulation also envisages that the Commission may develop non-binding model contractual terms. Such contractual standardisation may reduce uncertainty, but it must be designed carefully: if it becomes excessively burdensome or divergent across Member States, it may itself become a source of transaction costs.

Paragraph 5, finally, defines refusal as an exceptional outcome. The HDAB shall refuse access where access to the requested data would entail a serious risk of infringement of intellectual property rights, trade secrets or regulatory data protection and where that risk cannot be addressed through appropriate measures. Any refusal must be reasoned. The logic is therefore not that secrecy excludes access, but that access is denied only when proportionate preservation measures cannot sufficiently contain a serious risk.

Read as a whole, Article 52 proceduralises the conflict between openness and secrecy. It organises a sequence: notification by the holder, identification of the allegedly protected content, justification of the protection need, assessment by the HDAB, adoption of preservation measures, possible conditional access and, only in the last instance, refusal. This architecture avoids both extremes: a pure access model that disregards confidentiality and a pure secrecy model that allows trade secrets to become a general veto. Its effectiveness, however, depends on the quality of the procedure and on the institutional capacity of the bodies applying it.

Online First

ISSN 2281-5147

The practical difficulty lies in the fact that Article 52 entrusts HDABs with a mixed legal, technical and economic assessment. They must determine whether the claim is sufficiently specific, whether the information may plausibly be protected, whether the proposed safeguards are adequate and proportionate, whether the residual risk is serious and whether refusal is justified. This is not a merely administrative exercise. It requires expertise in intellectual property, data governance, health research, cybersecurity, anonymisation and secure processing environments, as well as the ability to balance public-interest access against legitimate commercial confidentiality.

5. Three implementation risks: overclaiming, expertise and fragmentation

The practical operation of this model raises three main concerns.

The first risk is overclaiming. Data holders may have incentives to invoke trade secret protection broadly in order to restrict access to datasets, delay disclosure, impose stricter conditions or preserve strategic control. This risk is not unique to the EHDS, but it is particularly relevant where data-sharing duties are imposed on actors that operate in competitive markets. If trade secret claims are accepted too easily, Article 52 may become a tool for narrowing the scope of secondary use.

Overclaiming may take different forms. A data holder may claim that an entire dataset is protected even where only specific elements are confidential. It may characterise ordinary organisational or technical choices as commercially valuable secrets. It may argue that disclosure would cause competitive harm without adequately demonstrating the seriousness of the risk. It may also use the complexity of the assessment to slow down access. The notification and justification requirement in Article 52(2) is therefore essential, but it will be effective only if HDABs are able to scrutinise claims critically.

The second risk concerns expertise. HDABs are expected to act as gatekeepers between data holders and data users. They must preserve protected interests while enabling access to the extent possible. This requires institutional capacity that may not be evenly distributed across Member States. Assessing the commercial value of a dataset, the risk of revealing confidential know-how, the adequacy of technical measures or the feasibility of anonymisation may require highly specialised knowledge.

Online First

ISSN 2281-5147

This concern has been raised by private stakeholders, especially in relation to early research datasets and innovation assets that are not protected by traditional intellectual property rights. From their perspective, excessive discretion in the hands of HDABs may create uncertainty and reduce incentives to establish or continue research activities in the EU. Industry stakeholders have argued that data holders should remain involved throughout the decision-making process and should retain effective control over intellectual property and trade secrets, including stronger possibilities to oppose access where disclosure would jeopardise protected assets[15]. While this argument should not be accepted uncritically, it highlights a real institutional challenge. The EHDS cannot rely on formal procedures alone. It needs competent, well-resourced and accountable bodies.

The third risk is fragmentation. The EHDS is a Regulation and is directly applicable, but its implementation depends on national institutions, operational rules and administrative practices. Member States will designate or establish HDABs and define aspects of their functioning within the boundaries of EU law. Divergent approaches to trade secret assessment, preservation measures, contractual terms, secure environments or refusal criteria may undermine the objective of a coherent European health data space. Fragmentation would be particularly damaging because the EHDS is premised on cross-border interoperability. If similar datasets are subject to different access conditions in different Member States, data users may face uncertainty and increased transaction costs. Data holders may engage in forum-sensitive strategies. Research projects may become more difficult to design. The result would be paradoxical: a Regulation intended to remove barriers to data sharing could generate new operational barriers through inconsistent implementation.

These three risks are connected. Overclaiming becomes more likely where institutional expertise is weak. Fragmentation becomes more likely where HDABs develop divergent practices in response to complex trade secret claims. Regulatory density may amplify both risks by making the applicable framework difficult to understand and costly to navigate.

[15] EFPIA, *Position on the Regulation on the European Health Data Space (EHDS)* <https://www.efpia.eu/media/2t2dem05/efpia-position-on-ehds.pdf>.

Online First

ISSN 2281-5147

6. EHDS within the broader European data law framework

The tension between openness and protected interests is not unique to the EHDS. It characterises the broader European data law framework. The Data Governance Act and the Data Act are particularly relevant because they also address access to data that may be protected by commercial confidentiality, intellectual property rights or trade secrets.

The Data Governance Act establishes rules for the reuse of certain categories of protected data held by public sector bodies. Article 3(1) DGA covers, among other categories, data protected on grounds of commercial confidentiality — including business, professional and company secrets — and data protected by third-party intellectual property rights. Recital 10 clarifies that commercial confidentiality includes trade secrets, protected know-how and other information whose undue disclosure would affect the market position or financial health of an undertaking[16]. The DGA therefore recognises that data reuse may involve confidential information and that protected status must be preserved. One of the mechanisms used by the DGA is the secure processing environment. Public sector bodies may require that access and reuse take place remotely within an environment provided or controlled by the public sector body[17]. This approach is relevant for the EHDS because secure processing environments may also serve as a technical and organisational response to trade-secret concerns. They can limit extraction, copying, re-identification and uncontrolled dissemination while still enabling analysis.

The Data Act also contains important rules on trade secrets[18]. Its objective is to create harmonised rules on fair access to and use of data, especially in relation to connected products and related services[19]. Recital 31 states that data holders should not be able

[16] See Louisa Specht-Riemenschneider, 'Article 3: Categories of Data' in Louisa Specht-Riemenschneider and Moritz Hennemann (eds), *Data Governance Act: Article-by-Article Commentary* (Nomos 2025) 117, 127-29.

[17] Regulation (EU) 2022/868, art 5(3)(b).

[18] For an introduction, see Moritz Hennemann, Gordian Kostatin Ebner, Benedikt Karsten, Gregor Lienemann and Marie Wienroeder, *Data Act: An Introduction* (Nomos 2024).

[19] On the broader IoT background of the Data Act, see Guido Noto La Diega, *Internet of Things and the Law: Legal Strategies for Consumer-Centric Smart Technologies* (Routledge 2023).

ISSN 2281-5147

to refuse data access solely because data are considered trade secrets. Articles 4(6) and 5(9) provide that trade secrets shall be disclosed only where necessary and only where all specific necessary measures are taken to preserve confidentiality. In exceptional circumstances, disclosure may be refused where the data holder is highly likely to suffer serious economic damage from the disclosure of trade secrets. The Data Act is relevant for at least two reasons. First, it shows that EU data law increasingly treats trade secrets as interests to be preserved rather than automatic barriers to access. Secondly, it reveals a general pattern: access obligations are accompanied by safeguards, proportionality assessments and exceptional refusal mechanisms. This pattern is also visible in the EHDS, though with sector-specific institutional arrangements. The literature on the Data Act has described this development as the emergence of a specific trade-secret framework for data access, one that may reshape the balance between control and circulation in the data economy[20].

Compared with the DGA and the Data Act, Article 52 EHDS is more sector-specific and institutionally demanding. The DGA relies on controlled reuse mechanisms for protected data held by public sector bodies, while the Data Act develops a more general access model in which trade secrets must be preserved but cannot normally operate as an automatic refusal ground. Article 52 EHDS follows the same direction, treating secrecy as an interest to be managed rather than as a veto. However, the EHDS model is more problematic because HDABs must assess trade-secret claims in a highly sensitive and technically complex health-data environment. The EHDS model has the advantage of entrusting these assessments to specialised access bodies, but its effectiveness will depend on whether those bodies have comparable expertise and develop sufficiently consistent practices across Member States.

At the same time, the multiplication of instruments creates coordination problems. GDPR, Open Data Directive, DGA, Data Act, AI Act and EHDS all contribute to the European data law landscape[21]. In the health sector, additional rules on clinical

[20] On the Data Act's treatment of trade secrets, see Ulla-Maija Mylly, 'Trade Secrets and the Data Act' (2024) 55 IIC 368; Ella De Noyette, Leander Stähler and Thomas Margoni, 'Data Secrets: The Data Act's New Trade Secrets Framework' (2025) 56 IIC 984; Moritz Hennemann, Gordian Kostatin Ebner, Benedikt Karsten, Gregor Lienemann and Marie Wienroeder, *Data Act: An Introduction* (Nomos 2024) 96-99, 109-10.

[21] On the reconstruction of European data law as a field that encompasses but extends beyond data protection law, see Thomas Streinz, 'The Evolution of European Data Law' in Paul Craig and

ISSN 2281-5147

trials, medical devices, cross-border healthcare and electronic communications may also be relevant. This regulatory density may produce what can be called a "regulatory fog": a situation in which the number and complexity of rules increase uncertainty and transaction costs, thereby discouraging the very data sharing that the strategy seeks to promote[22].

The regulatory fog is not simply a problem of excessive legislation. It is a problem of translation between narrative and operational rules. At the narrative level, the EU promotes openness, data sharing, common data spaces and public-interest innovation. At the operational level, actors must navigate overlapping legal regimes, national implementation choices, institutional discretion, trade secret claims, contractual safeguards and technical constraints. The gap between these levels is where many data-sharing projects fail.

Recent simplification initiatives, including the Digital Omnibus package, confirm that the coordination of EU digital legislation has become a regulatory problem in its own right. The package is not a single text but a set of initiatives. The general Digital Omnibus proposal, aimed at simplifying the digital legislative framework, remained in the ordinary legislative procedure at the time of writing, whereas the AI-related proposal had reached a provisional agreement between the Council presidency and the European Parliament on 7 May 2026 and still required formal adoption before entry into law. For the purposes of this article, that debate is relevant not because it has already modified Article 52 EHDS, but because it confirms the need to read sectoral data spaces through the lens of operational coherence. Simplification, however, cannot be equated with deregulation: reducing overlaps and clarifying

Gráinne de Búrca (eds), *The Evolution of EU Law* (3rd edn, OUP 2021) 902. On the continued centrality of EU data protection law in the EU digital rulebook, see Gabriela Zanfir-Fortuna, 'Follow the (Personal) Data: Positioning Data Protection Law as the Cornerstone of the EU's Fit for the Digital Age Legislative Package' (working paper, forthcoming in EDPS at 20 Anniversary Volume, June 2024) <https://ssrn.com/abstract=4794182>.

[22] For a different view of the broader relationship between digital regulation and innovation, see Anu Bradford, 'The False Choice Between Digital Regulation and Innovation' (2024) 119 Northwestern University Law Review 377. Bradford rejects the claim that the EU-US technology gap should be primarily attributed to the stringency of EU digital regulation and points instead to structural factors such as fragmentation of the digital single market, weaker capital markets, bankruptcy law, risk culture and talent attraction. She also stresses that digital regulation may redirect innovation towards social goals such as privacy, safety, trust and fairness.

Online First

ISSN 2281-5147

interfaces between instruments should not weaken the safeguards that make health-data reuse legitimate and trustworthy[23].

7. Legal interoperability, comparative approach and the operational turn

Interoperability is often used as if it were a purely technical concept. In the EHDS, technical interoperability is undoubtedly indispensable: systems must be able to exchange data through compatible formats, infrastructures, security requirements and standards. Semantic interoperability is equally important, because data must be understood in the same way by different systems and actors. Organisational interoperability is also necessary, since institutions must align procedures, responsibilities and workflows. Yet none of these dimensions is sufficient where the legal conditions for access remain uncertain, fragmented or difficult to operationalise[24].

Legal interoperability adds this further layer. It concerns the capacity of actors operating under different legal frameworks to cooperate without legal barriers that make data sharing uncertain, unsafe or impracticable. In the context of Article 52 EHDS, this requires clarity on the identification of protected content, the justification of trade-secret claims, the authority competent to assess them, the safeguards that may be imposed, the circumstances in which access may be refused and the remedies

[23] European Commission, Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus) COM(2025) 837 final; European Commission, Proposal for a Regulation as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI) COM(2025) 836 final; EDPB-EDPS, Joint Opinion 2/2026 on the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus) (10 February 2026). On the state of the procedure, see European Parliament, Legislative Train Schedule, 'The Digital Omnibus Regulation Proposal', procedure 2025/0360(COD), status 'Tabled' (as of 20 April 2026); Council of the European Union, 'Artificial Intelligence: Council and Parliament Agree to Simplify and Streamline Rules' (Press Release, 7 May 2026).

[24] On the multidimensional nature of interoperability, see ISO/TS 27790:2009, Health informatics - Document registry framework; European Commission, New European Interoperability Framework - Promoting Seamless Services and Data Flows for European Public Administrations (Publications Office 2017); EHDS Regulation, art 2(1)(f).

ISSN 2281-5147

available to the parties involved. Legal interoperability is therefore not an abstract value. It is an operational condition for cross-border secondary use[25].

This methodological lens also helps to frame the specific contribution of Article 52. The issue is not whether the EHDS can eliminate the conflict between openness and secrecy, but whether it can convert trade-secret protection into a manageable access condition. A secrecy claim should not produce radically different effects across Member States merely because HDABs develop divergent practices, require different contractual safeguards or apply different thresholds for serious risk. If that occurred, the EHDS would remain formally harmonised but operationally fragmented.

Legal interoperability can be pursued through a combination of techniques. Harmonisation provides common rules and minimum obligations. Standardisation may translate those rules into reusable procedures, technical specifications, metadata requirements, secure-processing protocols and model contractual clauses. Mutual recognition may become relevant when decisions, safeguards or access conditions adopted in one Member State must be trusted by authorities, data holders or data users in another. None of these techniques is sufficient in isolation. Taken together, however, they can reduce the legal transaction costs that would otherwise discourage data sharing[26].

Article 52 should therefore be implemented through a set of common legal-operational expectations. Data holders should identify the allegedly protected components of a dataset with sufficient precision, avoiding generic claims over whole data collections where only specific layers, annotations, methods, curation practices

[25] See Paolo Guarda, 'Sulla necessità di una visione ricostruttiva dell'approccio alla condivisione dei dati sanitari ed il ruolo dell'interoperabilità (giuridica)' (2026) 1 Persona e Mercato 61, 75-82, where legal interoperability is framed as both a systemic tool and a terminological bridge between legal and technical-informational knowledge in the context of health-data sharing; Rolf H Weber, 'Legal Interoperability as a Tool for Combatting Fragmentation', Global Commission on Internet Governance Paper Series No 4 (2014) 4-9; Urs Gasser and John Palfrey, 'Fostering Innovation and Trade in the Global Information Society: The Different Facets and Roles of Interoperability' in Mira Burri and Thomas Cottier (eds), *Trade Governance in the Digital Age* (Cambridge University Press 2012) 123-153.

[26] Weber (n. 25) 7-9; Odile Graber-Soudry, Timo Minssen, Daniel Nilsson, Marcelo Corrales, Jacob Wested and Bastian Illien, *Legal Interoperability and the FAIR Data Principles* (EOSC Study, 2021) 18-23; Chryssoula Doldirina, Aaron R Eisenstadt, Harlan Onsrud and Paul F Uhlir, *Legal Approaches for Open Access to Research Data* (2018).

ISSN 2281-5147

or processing pipelines require protection. HDABs should use comparable criteria to assess commercial value, secrecy measures and the risk of disclosure. Preservation measures should be proportionate and modular, ranging from contractual confidentiality obligations to access controls, secure processing environments, output checking and restrictions on onward disclosure. Refusal should remain a reasoned last resort[27].

At this point, the comparative approach becomes relevant. The EHDS operates within a legal and institutional environment in which health-data governance crosses borders, legal systems, technical infrastructures and administrative cultures. Clinical research networks, AI development, cloud infrastructures, cross-border healthcare and public-health emergencies do not stop at national boundaries. Comparative law is useful not because it offers a catalogue of foreign models to be transplanted, but because it helps identify how similar policy objectives are translated into different operational rules. It can reveal whether divergences are substantive or merely terminological, whether apparently different models produce equivalent safeguards, and whether national implementation choices create avoidable barriers to cooperation[28].

A comparative perspective remains relevant even within a framework largely governed by EU Regulations. Regulations provide formal uniformity, but they do not remove all differences in institutional design, administrative practice, enforcement culture, technical capacity and national healthcare infrastructures. In the EHDS, Member States will still designate or establish HDABs, organise their functioning and embed access procedures within pre-existing legal and technical systems. This perspective is therefore not used to examine autonomous national substantive rules, but to assess how a formally uniform EU framework is translated into different operational settings and whether those differences remain compatible with legal interoperability.

---

[27] On the need to make access conditions machine-actionable and reuse-oriented where legal restrictions apply, see Mark D Wilkinson, Michel Dumontier, IJsbrand J Aalbersberg and others, 'The FAIR Guiding Principles for Scientific Data Management and Stewardship' (2016) 3 Scientific Data 160018; Graber-Soudry and others (n. 26).

[28] For the comparative-law background, see Rodolfo Sacco and Piercarlo Rossi, *Introduzione al diritto comparato*, in Rodolfo Sacco (ed), *Trattato di diritto comparato* (UTET 2024) 55-70, 123-139.

ISSN 2281-5147

This is particularly important in a field where legal innovation is still unsettled. Data spaces, secure processing environments, algorithmic development, health-data altruism and secondary use are concepts that circulate between legal systems before their effects are fully stabilised. The comparatist is therefore not only concerned with differences and similarities between legal orders, but also with the circulation of models, the transformation of legal categories and the institutional conditions under which rules become workable. In this sense, the EHDS is not merely an object of sectoral health-data regulation. It is also a laboratory for observing how European data law attempts to govern technological and institutional complexity through common legal infrastructures[29].

The same perspective is useful when considering the European debate on digital sovereignty. Digital sovereignty is often invoked as Europe's ability to act independently in the digital environment and to preserve European values in global data markets. As a political narrative, it helps explain the EU's preference for common infrastructures, sector-specific data spaces and a rights-oriented model of digital regulation. As a legal category, however, it remains imprecise. In the EHDS, sovereignty becomes meaningful only when translated into access procedures, institutional responsibilities, secure environments, rights of data subjects, confidentiality safeguards and remedies[30].

A similar caution is necessary with the language of innovation. The EHDS aims to support scientific research, public health, digital medicine and AI systems. These objectives are legitimate and important, but innovation cannot become a rhetorical trump card that pushes rights and safeguards into the background. Safeguards are not external obstacles to innovation; in sensitive sectors such as health, they are

[29] Giovanni Smorto, 'Il ruolo della comparazione giuridica nella contesa per la sovranità digitale' (2023) 57(1) DPCE Online 339, 339-369. See also Thomas Streinz, 'The Evolution of European Data Law' in Paul Craig and Gráinne de Búrca (eds), *The Evolution of EU Law* (3rd edn, Oxford University Press 2021) 902-936.

[30] Teresa Madiega, *Digital Sovereignty for Europe* (European Parliamentary Research Service 2020); Luciano Floridi, 'The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU' (2020) 33 Philosophy & Technology 369; Giusella Finocchiaro, 'La sovranità digitale' (2022) 3 Diritto pubblico 809; Giorgio Resta and Federico Simonetti, 'La c.d. sovranità digitale e il progetto Gaia-X' (2022) 3 Contratto e impresa Europa 479; Huw Roberts, 'Digital Sovereignty and Artificial Intelligence: A Normative Approach'(2024) 26 Ethics and Information Technology.

ISSN 2281-5147

conditions for trustworthy innovation. The reverse is also true: trade secrets cannot become a rhetorical trump card that transforms every commercially valuable dataset into a closed door[31].

Legal interoperability also has an interdisciplinary function. Trade-secret risks cannot be evaluated by legal definitions alone. They depend on how datasets are structured, curated, labelled, linked, accessed and processed. Conversely, technical safeguards cannot be designed without legal choices about proportionality, accountability, confidentiality and purpose limitation. In this sense, legal interoperability operates as a boundary concept: it allows lawyers, technologists, data holders, HDABs and researchers to work on the same problem without assuming that one disciplinary vocabulary can replace the others[32].

The point, then, is to move from the declamatory level to the operational level. Narratives open the policy debate: openness, sovereignty, innovation, trust, European values. Operational rules determine whether data will actually circulate. Article 52 EHDS is a useful case study because it shows that the fate of secondary use may depend on institutional and procedural choices that are apparently technical but legally decisive: the design of forms, the content of justifications, the expertise of HDABs, the wording of contractual clauses, the structure of secure environments and the quality of reasons given for refusal.

The practical implication is straightforward. The EHDS will succeed only if it makes lawful sharing easier than non-sharing. If the legal path to access is too uncertain, slow or fragmented, actors will default to caution. If, on the contrary, access ignores legitimate confidentiality interests, trust and investment may be weakened. Legal

[31] On the relationship between digital regulation and innovation, cautioning against the view that EU digital regulation as such explains Europe's technological lag, see Anu Bradford, 'The False Choice Between Digital Regulation and Innovation' (2024) 119 Northwestern University Law Review 377, 382-383, 419-450. Bradford argues that the EU-US technological gap is better understood by considering structural factors such as market fragmentation, capital markets, risk culture and talent attraction.

[32] On boundary objects and interdisciplinary methods, see Julie Thompson Klein, Beyond Interdisciplinarity: Boundary Work, Communication, and Collaboration (Oxford University Press 2021) 15-25. For an application of this idea to legal interoperability as a bridge between legal and technical-informational knowledge, see Guarda (n. 32) 81-82.

ISSN 2281-5147

interoperability is the condition that can prevent both outcomes: it should make secrecy governable without allowing secrecy to govern the data space.

8. Conclusion: Jekyll, Hyde and the discipline of operational rules

The EHDS embodies a structural duality. It is animated by the promise of openness, but it must operate in an environment shaped by secrecy, commercial value and strategic control. It seeks to enable scientific research, public health and AI innovation, but it must also preserve legitimate interests of data holders and innovators. It promotes data sharing, yet it can do so only through controlled access, institutional assessments and technical safeguards.

This duality recalls the well-known line from Robert Louis Stevenson's Strange Case of Dr Jekyll and Mr Hyde: "*man is not truly one, but truly two*". It is useful because it captures the dual form of the EHDS: a project of openness and a system of controlled access; an infrastructure for public-interest reuse and a framework that recognises private value; a promise of interoperability and a possible source of fragmentation[33].

Article 52 is the provision in which this duality becomes operational. It confirms that electronic health data protected by intellectual property rights, trade secrets or regulatory data protection shall be made available for secondary use. At the same time, it requires preservation measures and allows refusal where access would entail a serious risk for protected interests. The point is that it assigns institutions the difficult task of governing coexistence between sharing and secrecy.

For that task to be credible, trade-secret claims must be made precise, reviewable and proportionate. Overclaiming must be controlled. HDABs must have access to legal, technical and economic expertise. Secure processing environments must be reliable. Contractual terms must reduce uncertainty rather than multiply it. Refusal decisions must remain exceptional and reasoned. National implementation must avoid turning Article 52 into twenty-seven different procedural cultures.

The contribution of legal interoperability is therefore specific. It does not replace technical interoperability, nor does it offer a general theory of European data law. It

[33] Robert Louis Stevenson, Strange Case of Dr Jekyll and Mr Hyde (1886) ch 10.

ISSN 2281-5147

provides the method for translating the EHDS promise into workable access conditions. In the field of trade secrets, this means making confidentiality compatible with reuse and making reuse compatible with legitimate confidentiality. The success of the EHDS will depend on whether this translation can be achieved in practice.

The European Data Strategy will ultimately be judged not by its slogans, but by the operational rules that make data sharing possible. The task is therefore not to choose between Dr Jekyll and Mr Hyde. Unlike Stevenson's story, Europe still has the possibility of writing a different ending: one in which openness and secrecy are not reconciled rhetorically, but governed through clear, balanced and interoperable rules.

Online First

ISSN 2281-5147