Essays

The Dual Configuration of the Right to Opt-Out in the European Health Data Space

Ana Menéndez Pérez*

ABSTRACT: This paper examines the dual configuration of the opt-out right within the framework of the European Health Data Space (EHDS). It analyses how this mechanism of data subject control assumes a distinct legal nature and regulatory regime depending on whether the processing is intended for the provision of healthcare or for scientific research, innovation, public health, and health policy-making. Through a doctrinal and normative analysis of the Regulation and its preparatory works, the paper explores the tensions between individual autonomy and the public interest in health data governance, highlighting the different balance struck between these competing interests under each regime.

KEYWORDS: opt-out right; European Health Data Space; primary use; secondary use; health data

SUMMARY: 1. Introduction – 2. The New Regulatory Ecosystem of the EHDS – 3. The Introduction of the Opt-Out Right in EHDS Governance – 4. The Opt-Out Right in the Primary Use of Health Data – 4.1. Exceptions – 4.2. Implementation Challenges – 5. The Opt-Out Right in the Secondary Use of Health Data – 5.1. Exceptions – 5.2. Implementation Challenges – 6. Synthesis Table of the Primary and Secondary Opt-Out Regimes – 7. Conclusions.

1. Introduction

In May 2022, when the European Commission presented its Proposal for a Regulation on the European Health Data Space (EHDS), European citizens had no mechanism by which to oppose the reuse of their electronic health data for research, innovation, or health policymaking purposes. Three years later, Regulation (EU) 2025/327[1] introduced an opt-out mechanism, but adopted a fundamentally different approach depending on whether the data were intended for primary or secondary use. This asymmetry – which reflects not merely a technical choice but a deliberate legislative policy decision concerning the balance between individual autonomy and the collective interest[2] – constitutes the central focus of this paper.

* *Predoctoral researcher, University of Basque Country (EHU). G.I.-CISJANT.- ref. IT1541-22, funded by the Department of Education of the Basque Government. Mail: ana.menendez@ehu.eus.* *This article was subject to a double-blind peer review process.*

[1] *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.*

[2] I. DE MIGUEL BERIAIN, M. LOYO MENOYO, *El Reglamento del Espacio Europeo de Datos de Salud ¿Qué podemos esperar?*, in *Gaceta Médica de Bilbao,* 122(1), 2025; P. TRIGO KRAMCSÁK, I. DE MIGUEL BERIAIN, *The Opt-Out Right for Secondary Uses of Personal Data in the European Health Data Space: Legal Basis, Scope, and Interplay with the GDPR*, in *Computer Law & Security Review*, 62, 2026, 106367.

Downloaded from https://teseo.unitn.it/biolaw
ISSN 2284-4503

The EHDS represents the first sector-specific regulatory framework of the European Union designed to govern the use and reuse of electronic health data across the Union, with a direct impact on healthcare practice and on the exploitation of data for biomedical research and innovation.[3] Its dual objective is clear: to empower individuals through effective control over their electronic health data[4] while facilitating their reuse for research, innovation, and public policymaking by overcoming the fragmentation and interoperability gaps that characterize the current framework.[5] At the heart of the EHDS regulatory architecture lies a structural distinction between the primary use – healthcare – and the secondary use – research, innovation, and public health – of electronic health data, each governed by a distinct legal regime.[6] It is precisely within that distinction that the opt-out right – the mechanism through which data subjects may express their wish that their data not be made available in certain EHDS contexts – assumes a fundamentally different legal nature and scope.[7]

In the primary use domain, the opt-out right is discretionary for Member States, which may or may not incorporate it into their domestic legal systems.[8] By contrast, in the secondary use domain, it is established as a subjective right, directly conferred on all Union citizens.[9] This divergence, combined with the broad margin of discretion left to Member States in implementing both regimes, may result in unequal levels of protection that are difficult to reconcile with the Regulation's objective of harmonization.[10] Although the General Data Protection Regulation[11] (GDPR) already recognizes the right to object,[12] the EHDS opt-out right is not its equivalent. Unlike the right to object, it operates preventively, without requiring any justification and with prospective effect, constituting a specific legal mechanism that strengthens the data subject's informational self-determination within the EHDS ecosystem.[13]

---

[3] I. De Miguel Beriain, M. Loyo Menoyo, *El Reglamento del Espacio Europeo de Datos de Salud*, cit.

[4] The Regulation, in line with the GDPR, recognizes and expands the rights of users over their health data, including the right to know the identity of those who access their electronic health record, the right to add data, the right to portability, and the right to limit or restrict access.

[5] P. Trigo Kramcsák, I. De Miguel Beriain, *The Opt-Out Right for Secondary Uses of Personal Data in the European Health Data Space*, cit.,2.

[6] D. Jove Villares, M. Presno Linera, *La salud en el entorno digital europeo*, in *Cuadernos Constitucionales*, 6, 89.

[7] P. Trigo Kramcsák, I. De Miguel Beriain, *The Opt-Out Right for Secondary Uses of Personal Data in the European Health Data Space*, cit.,6.

[8] As follows from Article 10(1) EHDS, "Member States' laws may provide that natural persons have the right to opt out". The use of the verb *may* indicate that the recognition of the opt-out right for primary use is optional and left to the discretion of the Member States.

[9] As follows from Article 71(1) EHDS, "Natural persons shall have the right to opt out at any time, and without providing any reason, from the processing of personal electronic health data relating to them for secondary use". The use of the mandatory verb shall demonstrate that the opt-out right for secondary use is directly recognized by the Regulation as a fully-fledged subjective right applicable throughout the Union, leaving Member States responsible only for establishing the mechanism through which that right may be exercised pursuant to Article 71(2).

[10] Recitals 1 and 7 EHDS. Recital 1 states that the Regulation aims to "improve the functioning of the internal market by laying down a uniform legal and technical framework". Recital 7 underlines the need to "reduce fragmentation, heterogeneity and division, and to create a system that is user-friendly and intuitive in all Member States".

[11] *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)*.

[12] Article 21 GDPR.

[13] P. Trigo Kramcsák, I. De Miguel Beriain, *The Opt-Out Right for Secondary Uses of Personal Data in the European Health Data Space*, cit.,15.

Downloaded from https://teseo.unitn.it/biolaw ISSN 2284-4503

This paper systematically examines the legal configuration of the opt-out right under the EHDS. The central thesis is twofold: first, the normative duality reflects legislative policy choices with direct implications for fundamental rights, including data protection and the right to privacy; second, heterogeneity in national implementation may generate unequal levels of protection incompatible with the Regulation's objective of harmonization.[14]

Methodologically, the paper adopts a normative approach based on the systematic examination of the EHDS and its interaction with the GDPR, complemented by recent academic literature and by the preparatory works of the Regulation – in particular the negotiating mandates of the European Parliament and the Council – which enable a reconstruction of the legislative rationale underlying the solutions ultimately adopted.

The paper proceeds as follows. Section 2 delineates the new regulatory ecosystem established by the EHDS. Section 3 reconstructs the legislative process that led to the introduction of the opt-out right. Sections 4 and 5 examine its legal regime in the primary and secondary use domains respectively, including the applicable exceptions and the principal implementation challenges. Section 6 presents a synthesis table setting out the principal similarities and differences between the opt-out regimes governing the primary and secondary use of electronic health data. Section 7 sets out the conclusions.

2. The New Regulatory Ecosystem of the EHDS

The digitalization of healthcare systems has profoundly transformed the nature, volume, and potential of health information.[15] Electronic health data are among the most valuable assets for scientific progress, the improvement of healthcare systems, and biomedical innovation, while at the same time being among the most sensitive from the perspective of fundamental rights.[16] In this context, the European Union has embraced a governance strategy aimed at harnessing that potential without compromising citizens' privacy guarantees and informational self-determination. The EHDS represents the most ambitious expression of that commitment: it is the first sectoral data space promoted within the European Data Strategy, and the first to enter into force.[17]

Regulation (EU) 2025/327, in force since 26 March 2025, establishes a regulatory framework covering the full range of possible uses of electronic health data – from direct healthcare to biomedical research, healthcare system management, public policy, and even life and health insurance. In view of this diversity, the EHDS is structured around a fundamental distinction between two domains: the primary use and

[14] Recitals 1 and 7 EHDS, cit.

[15] OECD, *Health in the 21st Century: Putting Data to Work for Stronger Health Systems*, OECD Health Policy Studies, Paris, 2019, 15-17 and, on the incomplete character of that transformation in the health sector, 12. See also L. MARELLI *et al.*, *The European Health Data Space: Too Big to Succeed?*, in *Health Policy*, 135, 2023, 104861.

[16] F. DE MONTALVO JÄÄSKELÄINEN, *Una reflexión desde la teoría de los derechos fundamentales sobre el uso secundario de los datos de salud en el marco del Big Data*, in *Revista de Derecho Político*, 106, 2020, 239-266. See also C. STAUNTON, M. SHABANI, D. MASCALZONI, S. MEŽINSKA, S. SLOKENBERGA, *Ethical and Social Reflections on the Proposed European Health Data Space*, in *European Journal of Human Genetics*, 32(5), 2024, 498-505.

[17] L. MARKSCHIES, *The European Health Data Space: The Next Step in Data Regulation*, in *Digital Decade: New Challenges for Law and Technology*, 2025, 425-440.

Downloaded from https://teseo.unitn.it/biolaw ISSN 2284-4503

the secondary use of electronic health data. Each is governed by a specific processing regime and set of safeguards, although the datasets to which they apply remain closely interconnected.[18]

"Primary use" is defined as "the processing of electronic health data for the provision of healthcare, in order to assess, maintain or restore the state of health of the natural person to whom those data relate, including the prescription, dispensation and provision of medicinal products and medical devices, as well as for relevant social, administrative or reimbursement services".[19] In essence, it encompasses the processing of electronic health data for the provision of direct healthcare, with the aim of ensuring appropriate care for the patient within the clinical relationship.[20] Such data are generally collected and managed through the electronic health record, although other datasets may also provide information relevant to more precise and personalized care.[21] Chapter II of the EHDS governs this domain, limited to priority categories of electronic personal health data enumerated in Annex I.[22]

"Secondary use", by contrast, encompasses "any processing of electronic health data for the purposes set out in Chapter IV of this Regulation, other than the initial purposes for which they were collected or produced".[23] It covers the reuse of electronic health data – generally in anonymized or pseudonymized form – for purposes of collective interest: scientific research and innovation, public policy, public health protection, patient safety, personalized medicine, and official statistics, among others. Chapter IV of the Regulation establishes an exhaustive catalogue of uses and purposes permitted *ex lege*, set out in Article 53. It is worth noting that the wording of the secondary use definition in the final text underwent a significant change compared to the Commission's 2022 Proposal, which had explicitly referenced data "initially collected in the context of primary use" as well as data "collected for secondary use".[24]

The distinction between primary and secondary use is not merely conceptual. It determines the legal regime applicable to data subjects,[25] the obligations of the actors involved and, crucially, the configuration of the opt-out right. The underlying rationale of each domain differs. In the primary use domain, processing serves the protection of the data subject's own health – which justifies certain limits on individ-

[18] D. Jove Villares, M. Presno Linera, *La salud en el entorno digital europeo*, cit., 89.

[19] Article 2(2) (d) EHDS.

[20] See art. 16(1) of the *Spanish Patients' Autonomy Act* (Law 41/2002 of 14 November) that, says: the medical record constitutes an instrument "primarily intended to ensure the provision of adequate care to the patient"; SESPAS, *Informe Protección de datos personales y secreto profesional en el ámbito de la salud: una propuesta de normativa de adaptación al RGPD*, 2017, 52; A.S. Casanova Asencio, *Espacio Europeo de datos sanitarios, uso primario y autonomía del paciente*, in M.B. Andreu Martínez (ed.), *Los datos de salud como eje de la transformación digital de la sanidad*, Granada, 2023, 118.

[21] S. Navas Navarro, *Datos sanitarios electrónicos. El espacio europeo de datos sanitarios*, Madrid, 2023, 50 ff.

[22] Article 14 and Annex I EHDS.

[23] Article 2(2) e) EHDS.

[24] I. De Miguel Beriain, *El uso de datos de salud para investigación biomédica a la luz de la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el Espacio Europeo de Datos Sanitarios*, in *Revista Jurídica de Castilla y León*, 60, 2023, 13-14; M. Recuero Linares, *El uso secundario de datos de salud electrónicos: el futuro del Reglamento del Espacio Europeo de Datos de Salud y su interacción con la protección de datos personales*, in *InDret*, 2, 2024, 11.

[25] Articles 2(1)(a) and 2(2)(a) EHDS. The Regulation does not provide an autonomous definition of the data subject but incorporates the definition laid down in Article 4(1) GDPR. In the context of secondary use, health professionals may also qualify as data subjects where their professional data form part of the electronic health datasets made available (Article 51(1)(j) EHDS).

Downloaded from https://teseo.unitn.it/biolaw ISSN 2284-4503

ual autonomy in the interest of continuity of care.[26] In the secondary use domain, electronic health data serve interests extending beyond the individual sphere, requiring a more careful balance between the collective value of the reuse data and the rights of the data subject.[27]

The EHDS ecosystem involves multiple actors. Data holders – including hospitals, clinics, public authorities, pharmaceutical companies, and other entities –[28] are required to make the relevant electronic health data available to national Health Data Access Bodies (HDABs),[29] which act as intermediaries between data holders and authorized health data users. Once granted the relevant data access permit, the latter may access and use the data only within secure processing environments, with access generally limited to anonymized data and, exceptionally, to pseudonymized data.[30] This governance architecture seeks to overcome the shortcomings of the previous framework, characterized by the regulatory fragmentation resulting from the uneven implementation of the GDPR across Member States, which had created significant obstacles for cross-border biomedical research.[31]

The EHDS does not create the data subject's rights from scratch. The GDPR already recognizes access, rectification, erasure, portability, and objection rights, all of which the Regulation preserves and integrates.[32] The EHDS additionally introduces new rights tailored to the digital health ecosystem, chief among which is the opt-out right. Its nature, scope, and legal regime vary substantially depending on the type of use involved, as the following sections demonstrate.

---

[26] Article 2(2)(d) EHDS defines primary use as the processing of electronic health data for the provision of healthcare in order to assess, maintain or restore the state of health of the natural person to whom those data relate. As regards continuity of care as the rationale underlying professional access, see Recital 19 EHDS. On the resulting limitations on individual autonomy, see Recital 17 EHDS, which recognizes that the unavailability of restricted data may affect the provision or quality of healthcare and that such restrictions may have life-threatening consequences. Accordingly, access must remain possible where necessary to protect the vital interests of the data subject or another natural person in emergency situations.

[27] I. DE MIGUEL BERIAIN, M. LOYO MENOYO, *El Reglamento del Espacio Europeo de Datos de Salud*, cit.

[28] Article 2(2)(t) EHDS. The concept of health data holder encompasses any natural or legal person, public authority, agency or other body in the healthcare or care sector, including reimbursement services where relevant, as well as entities developing products or services for the health sector, wellness applications, or conducting health-related scientific research. It therefore includes, inter alia, hospitals, clinics, public bodies, pharmaceutical companies, manufacturers of medical devices, developers of wellness applications, nursing homes, day-care centres and providers of care services (see also Recital 59 EHDS).

[29] Health Data Access Bodies are designated by the Member States pursuant to Article 55 EHDS. Their tasks, including receiving data from health data holders and making them available for authorized secondary use, are set out in Article 57 EHDS. Health data holders are required, upon request, to make the electronic health data referred to in Article 51 available to the relevant Health Data Access Body pursuant to Article 60(1) EHDS.

[30] European Commission, *Frequently Asked Questions (FAQs) on the European Health Data Space*, 5 March 2025.

[31] M. SALOKANNEL, *Opting-in or -out or Not at All: Secondary Use of Health Data in the EHDS Framework*, in *European Law Blog*, 2024, https://europeanlawblog.eu/ghb7e7wu/ (last visited 26/05/2026).

[32] Articles 15 (right of access), 16 (right to rectification), 17 (right to erasure), 20 (right to data portability) and 21 (right to object) GDPR. Article 1(4) EHDS provides that the Regulation is without prejudice to Regulation (EU) 2016/679, while Recital 8 states that the EHDS builds upon and complements the rights established under the GDPR as applied to personal electronic health data. Accordingly, Chapter II EHDS supplements the GDPR framework by introducing additional rights specific to electronic health data, including the rights laid down in Articles 3 and 5 to 10 EHDS.

Downloaded from https://teseo.unitn.it/biolaw ISSN 2284-4503

Before examining the opt-out right in each of those domains, however, it is necessary to reconstruct the legislative process that led to its introduction, since the institutional tensions that emerged during that process largely explain the dual configuration ultimately adopted by the Regulation.

3. The Introduction of the Opt-Out Right in EHDS Governance

The Commission's original proposal, presented in May 2022, made no provision for an opt-out right in the secondary use domain.[33] The governance architecture initially designed proceeded on the premise that the system's own safeguards – secure processing environments and mandatory HDAB intermediation[34] – were sufficient to protect data subjects, whose rights would be residually covered by the GDPR and, in particular, by the right to object under Article 21.[35]

This initial configuration generated an intense institutional debate, one of the most contentious aspects of the entire legislative process.[36] The positions of the Parliament, the Council, and the Commission diverged significantly on the degree of individual control to be recognized over the secondary use of health data.[37]

---

[33] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space*, COM(2022) 197 final, 3 May 2022.

[34] Secure processing environments (SPEs) are the controlled technical environments through which health data access bodies provide access to electronic health data for secondary use. Rather than defining the concept, Article 73 EHDS establishes its functional requirements by providing that access under a data permit may take place only through such environments and subject to technical, organizational, security and interoperability requirements. Article 73(2) further requires health data access bodies to ensure that only non-personal electronic health data, including anonymized statistical data, may be extracted from those environments. HDAB intermediation refers to the central role of health data access bodies as the exclusive gateway for access to electronic health data for secondary use: health data holders must make the relevant data available to the competent health data access body upon request (Article 60(1) EHDS), while health data users may obtain access only through a data permit issued pursuant to Article 68 EHDS or an approved health data request under Article 69 EHDS, following an application submitted under Article 67 EHDS. On the designation and tasks of health data access bodies, see Articles 55 and 57 EHDS.

[35] M. SALOKANNEL, *Opting-in or -out or Not at All*, cit.

[36] M. SALOKANNEL, *Opting-in or -out or Not at All*, cit.

[37] Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, COM(2022) 197 final, 3 May 2022, which did not provide for an opt-out right in relation to the secondary use of electronic health data, relying instead on the safeguards embedded in the proposed governance framework and on the rights guaranteed under Regulation (EU) 2016/679, while Article 33(5) referred the question of consent to national law. Council of the European Union, *Mandate for negotiations with the European Parliament on the European Health Data Space*, doc. ST 16048/23 REV 1, 7 December 2023, adopted as the Council's general approach on 6 December 2023, which made the introduction of an opt-out mechanism optional, leaving Member States the discretion to introduce and shape such a right in light of their legal traditions, historical experience and national circumstances. European Parliament, *European Health Data Space – Amendments adopted on 13 December 2023 on the proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space*, P9_TA(2023)0462 (COM(2022)0197 – C9-0167/2022 – 2022/0140(COD)), OJ C, C/2024/4200, 2 August 2024, which proposed the introduction of an opt-out right for natural persons in respect of the secondary use of their electronic health data, directly conferred by the Regulation itself rather than left to the discretion of the Member States. The compromise reached during the trilogue negotiations on 15 March 2024 was subsequently reflected in the European Parliament's first-reading position of 24 April 2024, P9_TA(2024)0331, and ultimately became Article 71 EHDS. See also EDPB–EDPS, *Joint Opinion 03/2022 on the Proposal for a Regulation on the Euro-*

Downloaded from https://teseo.unitn.it/biolaw ISSN 2284-4503

The Council, in its negotiating mandate, favored a stance of deference to Member States.[38] The Council considered that any right to object beyond Article 21 GDPR should be optional and left to each national legal order, on the grounds that the balance between individual autonomy and data availability for secondary uses was a matter "best made at national level, taking into account Member States' specific situations and historical experiences".[39] Had this position prevailed, it would have reproduced within the EHDS the same regulatory fragmentation already characterizing the uneven application of the GDPR on health data across the Member States.[40]

The European Parliament, by contrast, advocated a general and uniform opt-out for all secondary uses of electronic health data, with the exception of human genetic, genomic, and proteomic data, data from biobanks and data from wellness applications, for which it required explicit consent (*opt-in*).[41] This opt-out right was founded, in the Parliament's view, on the protection of the confidential relationship between patient and physician, as recognized by the European Court of Human Rights.[42] The parliamentary proposal also required HDABs to make detailed, easily accessible information publicly available on the conditions for secondary data use and on data subjects' rights and the remedies.[43]

Scholars have underlined the need to distinguish the opt-out mechanism from the GDPR right to object.[44] The right to object under Article 21 GDPR is conditional: it requires the data subject to invoke reasons relating to their particular situation and may be overridden where the controller demonstrates compelling legitimate grounds. In the field of scientific research, the right is further curtailed: under Article 21(6) GDPR it is excluded altogether where the processing is necessary for the performance of a task carried out for reasons of public interest. In practice, invoking the right to object requires the data subject to disclose personal – potentially sensitive – information as justification, which is particularly

---

pean Health Data Space, 12 July 2022, advocating stronger safeguards for data subjects and enhanced individual control over the secondary use of electronic health data.

[38] Council of the European Union, *Proposal for a Regulation on the European Health Data Space — Mandate for negotiations with the European Parliament*, doc. 16048/1/23 REV 1, 7 December 2023 (Interinstitutional File 2022/0140(COD)). The Council's deference to Member States is reflected in Recital 37a, which provides that Member States *may* introduce a specific right to object to the secondary use of electronic health data and remain free to determine whether and how to shape such a right in light of their specific national circumstances and historical experience.

[39] Council of the European Union, *Proposal for a Regulation on the European Health Data Space — Mandate for negotiations with the European Parliament*, cit., Recital 37a.

[40] M. SALOKANNEL, *Opting-in or -out or Not at All*, cit. See also DG Sante, *Assessment of the EU Member States' Rules on Health Data in the Light of GDPR*, Brussels, 2021.

[41] European Parliament, *European Health Data Space — Amendments adopted on 13 December 2023 on the proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space*, P9_TA(2023)0462 (COM(2022)0197 – C9-0167/2022 – 2022/0140(COD)), OJ C, C/2024/4200, 2 August 2024, Amendment 39 (Recital 39a).

[42] ECtHR, *Z. v. Finland*, 25 February 1997.

[43] European Parliament, *European Health Data Space – Amendments adopted on 13 December 2023*, cit., Article 38. On medical confidentiality as the foundation of the secondary use debate, see D. SPAJIĆ, *Transforming the Secondary Use of Patient Data in the European Health Data Space: A Challenge for the Patient's Right to Medical Confidentiality?*, in S. SLOKENBERGA, K.Ó CATHAOIR, M. SHABANI (eds.), *The European Health Data Space. Examining a New Era in Data Protection*, Abingdon-New York, 2025, 87-109.

[44] See M. KRUUS, *Opting Out of Scientific Research with Health Data: The Limits of the EHDS and the GDPR*, in *European Journal of Health Law*, 32(2), 2025, 165-189.

Downloaded from https://teseo.unitn.it/biolaw ISSN 2284-4503

problematic for health data.[45] The opt-out, by contrast, enables exclusion from the secondary use system without justification, without disclosing additional information, and with prospective effect.[46]
The final text, Regulation (EU) 2025/327, largely reflected the Parliament's position[47] as regards secondary use, although it did not retain the opt-in mechanism proposed for particularly sensitive categories of data. Instead, it introduced the opt-out right as a full subjective right under Article 71, directly conferred on all Union citizens in relation to the secondary use of electronic health data. As regards primary use, Article 10 adopted a discretionary approach, leaving the introduction of the opt-out mechanism to the Member States, in line with the concerns expressed by the Council during the negotiations.[48] This compromise reflects the persistent tension between the Parliament's harmonizing vision and the Council's preference for national discretion – a tension that was not fully resolved in the final text of the Regulation.

4. The Opt-Out Right in the Primary Use of Health Data

Chapter II of the EHDS governs the processing of electronic health data for healthcare purposes. Its scope is not unlimited, however, but confined to the priority categories of personal electronic health data listed in Annex I.[49] Among the rights recognized in this framework is the opt-out right.
In the primary use domain, Article 10 configures the opt-out right as an optional mechanism for Member States: its incorporation into domestic law is left entirely to their discretion. Where it is recognized, it enables natural persons to restrict access to their personal electronic health data recorded in an EHR system, through the access services provided for in the EHDS.[50]
In practical terms, the exercise of the right means that the data subject's personal electronic health data may not be made available, through the EHDS interoperable services such as MyHealth@EU, to parties

[45] M. Salokannel, *Opting-in or -out or Not at All*, cit.
[46] P. Trigo Kramcsák, I. De Miguel Beriain, *The Opt-Out Right for Secondary Uses of Personal Data in the European Health Data Space*, cit.,12.
[47] Article 71(1) EHDS confers the opt-out right directly on natural persons, who may exercise it at any time and without providing reasons; the exercise of the right is reversible. Article 71(2) further requires Member States to establish an accessible and easily understandable opt-out mechanism. This structure largely reflects the European Parliament's approach, under which the right was to be conferred directly by the Regulation rather than depend upon national implementation (P9_TA(2023)0462, Amendment 39 (Recital 39a)). It departs from the Council's negotiating position, which left the introduction and design of such a right to the discretion of the Member States (doc. 16048/1/23 REV 1, Recital 37a). The Parliament had also proposed that the secondary use of human genetic, genomic and proteomic data, together with data from biobanks and wellness applications, be subject to an opt-in mechanism based on the data subject's consent; this was not retained in the final text of Article 71.
[48] Article 10(1) EHDS provides that Member States may establish an opt-out mechanism for the primary use of electronic health data, thereby leaving its introduction to national discretion. Article 10(2) requires those Member States choosing to do so to lay down the rules and specific safeguards governing its operation. This configuration closely reflects the Council's negotiating position. Indeed, Recital 18 EHDS substantially reproduces Recital 13a of doc. 16048/1/23 REV 1, both attributing the discretionary approach to the differing sensitivities among Member States regarding the degree of patient control over electronic health data, both allowing an absolute opt-out without an emergency override, and both leaving the detailed rules and safeguards – including those relating to particular categories of data, such as genetic data – to national law.
[49] Article 14 and Annex I EHDS.
[50] Article 4 and 12 EHDS.

Downloaded from https://teseo.unitn.it/biolaw ISSN 2284-4503

other than the healthcare provider that originally recorded the data. Patient control over the sharing of clinical information within interoperable digital environments is thereby strengthened.[51]

Article 10 grants broad discretion to Member States both to decide whether to incorporate the right and to determine the specific conditions for its exercise. Recital 18 explains that this reflects the differences that exist between Member States regarding the degree of patient control over health data.[52] The practical implications of this margin of appreciation for the coherence of the internal market for health data are significant. Where the opt-out right is not recognized, or where it is afforded a more limited scope, citizens will enjoy substantially inferior informational autonomy compared to residents of States that have incorporated it in full. This regulatory asymmetry may erode trust in the system and compromise the harmonization the Regulation seeks to achieve.[53]

The exercise of the opt-out does not interrupt the functioning of the EHR system, which healthcare professionals continue to populate in the course of their clinical activities. Nor is the opt-out permanent: the data subject may revoke it at any time.[54] Data continue to be recorded and stored in local systems, remaining accessible to the providers that generated them.[55] The practical effect is to place the patient in a position comparable to the one that existed before the EHDS, characterized by the fragmentation of clinical information across different healthcare providers.[56]

The opt-out right must be distinguished from the right to restrict access.[57] The latter allows the total or partial restriction of data visibility within the EHR system. The opt-out, by contrast, excludes data from the interoperable exchange system as a whole. It should also be noted that the opt-out right may be ex-

[51] Article 10 EHDS, which empowers Member States to provide for a primary use opt-out in respect of access through the electronic health data access services referred to in Articles 4 and 12, and requires them to lay down the rules and specific safeguards governing the mechanism. The substantive content of the right is set out in Recital 18 EHDS: exercising it means that the personal electronic health data of the natural person concerned may not be made available, through the services set up under the EHDS, to anyone other than the healthcare provider that prescribed the treatment.

[52] See also M.J. Saks *et al.*, *Granular Patient Control of Personal Health Information: Federal and State Law Considerations*, in *Jurimetrics*, 58(4), 2018, 411-435.

[53] Empirical research shows that many individuals across the European Union have only limited awareness of the secondary uses made of their health data: See L.L. Skovgaard, S. Wadmann, K. Hoeyer, *A Review of Attitudes towards the Reuse of Health Data among People in the European Union: The Primacy of Purpose and the Common Good*, in *Health Policy*, 123(6), 2019, 564-571. At the same time, the literature on informational privacy demonstrates that the practical effectiveness of legal rights depends not only on their formal recognition but also on the design of default rules and the information available to individuals. see D. J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, in *Harvard Law Review*, 126(7), 2013, 1880-1903; A. Acquisti, L. Brandimarte, G. Loewenstein, *Privacy and Human Behavior in the Age of Information*, in *Science*, 347(6221), 2015, 509-514; and, on the determinative effect of defaults in a comparable health context, E. J. Johnson, D. Goldstein, *Do Defaults Save Lives?*, in *Science*, 302(5649), 2003, 1338-1339.

[54] E. Seijas Villadangos, *Desafíos del derecho a la protección de la salud en el proceso hacia su digitalización: equidad, sostenibilidad y progresividad*, in *Teoría y Realidad Constitucional*, 56, 2025, 250.

[55] European Commission, *Frequently Asked Questions (FAQs) on the European Health Data Space*, cit.

[56] See Recital 7 EHDS, describing the pre-existing fragmentation of electronic health data across healthcare providers, and Recital 18 EHDS, which acknowledges that the exercise of the primary-use opt-out may result in health professionals lacking access to information necessary for the continuity and quality of care.

[57] Article 8 EHDS, on the right to restrict access to personal electronic health data for primary use; see also Recital 17 EHDS.

Downloaded from https://teseo.unitn.it/biolaw ISSN 2284-4503

ercised in either domain – primary or secondary use – without the exercise in one automatically extending to the other.[58]

Reversibility is an unconditional requirement: Article 10(1) expressly provides that "Member States shall ensure that the exercise of that right is reversible". The data subject may therefore revoke the opt-out at any time, thereby restoring access through EHDS services. That said, reversibility does not guarantee that data generated during the opt-out period will automatically be integrated into the interoperable system, which may limit the practical scope of restoring access.[59]

4.1. Exceptions

The primary use opt-out does not operate in absolute terms. Article 10(2) allows Member States to establish exceptions where access is necessary to protect the vital interests of the data subject or another natural person, within the meaning of Article 9(2)(c) GDPR.[60] This provision reflects the primacy of the healthcare purpose: patient autonomy yields to the imperative of preserving life or physical integrity in emergency situations. Although the incorporation of this exception is not mandatory, its adoption appears functionally necessary to prevent the opt-out right from jeopardizing urgent medical care.[61]

A degree of normative tension is, however, introduced by Recital 18, which expressly contemplates the option for Member States to provide for the opt-out as an absolute right,[62] with no exceptions even in emergencies, acknowledging the differences between national legal orders regarding the degree of protection to be afforded to patient autonomy. This openness to an absolute configuration, combined with

[58] Articles 10 and 71 EHDS establish separate opt-out rights for primary and secondary use respectively, as defined in Article 2(2)(d) and (e). The Regulation contains no provision extending the exercise of one right to the other.

[59] Recital 18 EHDS "personal electronic health data generated during the period of the opt-out might not be available via the access services and MyHealth@EU".

[60] Art. 10(2) EHDS: "Member States may provide for a healthcare provider or health professional to be able to get access to the personal electronic health data in cases where processing is necessary in order to protect the vital interests of the data subject or of another natural person as referred to in Article 9(2) (c) of Regulation (EU) 216/679, even if the patient has exercised the right to opt out in primary use".

[61] Recital 17 EHDS states that restrictions on access to personal electronic health data may have life-threatening consequences and that access must therefore remain possible where necessary to protect vital interests in an emergency; the same logic underlies Article 10(2) EHDS. The exception is not an innovation of the EHDS: Article 9(2)(c) GDPR already lifts the prohibition on processing special categories of data where necessary to protect the vital interests of the data subject or of another natural person and the data subject is physically or legally incapable of giving consent, and Article 6(1)(d) GDPR does the same as a lawful ground, Recital 46 GDPR clarifying that reliance on the vital interests of another person is subsidiary to any other available legal basis. The concern that a merely optional exception may produce divergent outcomes is borne out by experience under the GDPR: Article 9(4) allowed Member States to maintain or introduce further conditions with regard to the processing of genetic, biometric and health data, and the resulting national divergence has been documented at Union level. See DG SANTE, *Assessment of the EU Member States' Rules on Health Data in the Light of GDPR*, Brussels, 2021. The cross-border dimension of the problem was expressly contemplated during the negotiations: the Council's mandate provided that an absolute right to object without an emergency override should be available both for cross-border access and for access internal to the Member State concerned (doc. 16048/1/23 REV 1, cit., Recital 13a). The practical stakes may be illustrated by a simple hypothetical: a patient who has exercised the primary use opt-out and suffers an anaphylactic reaction while travelling would, in a Member State that has implemented the exception, have the allergy recorded in their electronic health record retrieved by the emergency team, whereas in a Member State that has not, the same episode would be managed without that information.

[62] Recital 18 EHDS: "Member states should be able to provide for an absolute right to opt-out".

Downloaded from https://teseo.unitn.it/biolaw ISSN 2284-4503

the possibility of emergency exceptions, illustrates the broad margin of appreciation left to Member States and the diversity of solutions that may result.[63]

Member States are also free to provide for differentiated regimes for specific categories of particularly sensitive data, such as genetic data.[64] This regulatory latitude reflects varying national sensitivities regarding the balance between patient autonomy and healthcare needs, but equally constitutes a risk factor for the coherence of the EHDS as an integrated European data space.[65]

4.2. Implementation Challenges

The practical effectiveness of the primary use opt-out depends largely on how Member States implement it. Because Article 10(2) leaves the design of the mechanism to national law without prescribing its content, the issues examined below are not shortcomings of the Regulation but matters that it deliberately leaves to national implementation.[66] Four of these appear to be of particular significance.

The most structural is the risk of regulatory fragmentation. Since Article 10 leaves both the decision to incorporate the right and the determination of its conditions entirely to Member States, highly heterogeneous national solutions may be anticipated.[67] This expectation is supported not only by the wording of article 10, but also by previous experience under EU data protection law. Member States begin from markedly uneven positions as regards the maturity of their health data management systems, and the equivalent margin afforded by Article 9(4) GDPR has already produced documented divergence in the treatment of health data across national legal orders.[68] Where the opt-out right does not exist or is afforded a more limited scope, citizens will enjoy a significantly lower level of informational autonomy, for

[63] The tension originates in the legislative negotiations. The Commission's proposal provided only for the emergency override, now reflected in Recital 17 EHDS (COM(2022) 197 final, cit., Recital 13). The possibility of an absolute opt-out was introduced by the Council as in a new Recital 13a (doc. 16048/1/23 REV 1, cit.), which became, in substance, Recital 18 EHDS. The final text retains both approaches, leaving their reconciliation to the discretion of the Member States.

[64] Article 10(2), read in the light of Recital 18 EHDS, which clarifies that the national rules and specific safeguards governing the primary-use opt-out may relate to specific categories of personal electronic health data, including genetic data.

[65] Recital 18 EHDS explains the discretionary approach by reference to the differing sensitivities among Member States regarding the degree of patient control over electronic health data. On the resulting risk of fragmentation and its implications for the coherence of the EHDS, see M. SALOKANNEL, *Opting-in or -out or Not at All*, cit.

[66] Article 10(2) EHDS requires Member States introducing a primary use opt-out to lay down the rules and specific safeguards governing the mechanism. The Regulation does not prescribe their content, so the questions examined in this section fall to national law. Except where otherwise indicated, the difficulties identified below are inferences drawn from the wording of the relevant provisions rather than matters expressly settled by the Regulation.

[67] See section 4.1 above. The premise was expressly acknowledged during the negotiations: the Council attributed the discretionary solution to the differing sensitivities among Member States as to the degree of patients' control over their health data (doc. 16048/1/23 REV 1, cit., Recital 13a), a rationale retained in Recital 18 EHDS.

[68] That such divergence is not merely hypothetical is borne out by experience under Article 9(4) GDPR, which allowed Member States to maintain or introduce further conditions with regard to the processing of genetic, biometric and health data: see DG Sante, *Assessment of the EU Member States' Rules on Health Data in the Light of GDPR*, cit. On the uneven starting positions of national health data management systems and their preparedness to comply with the Regulation, see I. A. KESSISSOGLOU, S. M. COSGROVE, L. A. ABBOUD, P. BOGAERT, M. PEOLSSON, N. CALLEJA, *Are EU Member States Ready for the European Health Data Space? Lessons Learnt on the Secondary Use of Health Data from the TEHDAS Joint Action*, in *European Journal of Public Health*, 34(6), 2024, 1102-1108.

Downloaded from https://teseo.unitn.it/biolaw ISSN 2284-4503

the reasons examined in the preceding section. The resulting asymmetry does not merely erode trust: it reproduces within the EHDS the very fragmentation the Regulation was intended to overcome.[69]

A second challenge arises in cross-border and inter-territorial contexts. If a patient who has exercised the opt-out requires healthcare outside their State of residence, professionals cannot access their clinical information through the interoperable mechanisms established by the Regulation, potentially affecting continuity and quality of care – the very objective that underpins the primary use regime.[70] Although the Regulation does not expressly address this, it would be appropriate for the data subject to be clearly informed of these practical consequences prior to exercising the right, in terms comparable to those envisaged for the right to restrict access. That requirement is not stated in Article 10; it is inferred here from the parallel treatment of the two rights and from the transparency obligations that continue to apply under the GDPR.[71]

A third issue concerns the practical limits of reversibility. Recital 18 clarifies that data generated during the opt-out period might not be available through the access services and MyHealth@EU once the system is reactivated. Revocation therefore does not fully restore the previous situation: it leaves a permanent gap in the interoperable record corresponding to the period of exclusion. Since the Regulation neither acknowledges this consequence nor requires that it be communicated, the risk is that reversibility will be understood by data subjects as a complete return to the status quo ante, which it is not.[72]

Finally, the Regulation does not clarify whether healthcare professionals will be informed that a patient has exercised the opt-out right – unlike the case of the right to restrict access, for which it is expressly established that the restriction is not visible to professionals. This omission creates a significant interpretative gap, and the two possible readings carry opposite risks. If professionals are not informed, they may be unaware that relevant clinical information exists in the local record and act on an incomplete picture; if they are informed, the exercise of the right becomes visible in the clinical relationship, with the attendant risk of stigma that the express rule in Article 8 was designed to avoid.[73] The Regulation is

[69] On the legal uncertainty and unequal treatment of data subjects likely to result from leaving these questions to national law, see M. SALOKANNEL, *Opting-in or -out or Not at All*, cit.

[70] Recital 19 EHDS identifies full and timely access by health professionals to patient records as fundamental to ensuring continuity of care, avoiding duplication and errors, and reducing costs, and notes that where such access is lacking health professionals cannot make optimal diagnostic and treatment decisions.

[71] Article 8 EHDS provides that natural persons restricting access are to be made aware that doing so might affect the healthcare provided to them, and Recital 17 EHDS adds that they are to be informed of the patient safety risks associated with restricting access to health data before the restriction is imposed. No equivalent provision accompanies Article 10. The requirement proposed here is therefore an inference drawn from the parallel treatment of the two rights, and from Articles 13 and 14 GDPR, which continue to apply within the EHDS framework by virtue of Article 1(4) and Recital 8 EHDS. On the centrality of comprehensible information to the effective exercise of rights of this kind, see P. CERVERA DE LA CRUZ, T. LALOVA-SPINKS, M. SHABANI, *The European Health Data Space: an opportunity to strengthen citizen rights and engage citizens in health data governance*, in *Frontiers in Medicine*, 12, 2026, 1699941.

[72] Recital 18 EHDS, according to which, where a natural person reverses an opt-out, personal electronic health data generated during the opt-out period might not be available through the access services or MyHealth@EU. The Regulation says nothing about how that consequence is to be communicated to the data subject either before the right is exercised or upon its reversal; the assessment of its practical significance offered here is the author's inference from the wording of that recital.

[73] The contrast is express. Article 8 EHDS provides that the fact that a natural person has restricted access is not to be visible to healthcare providers, whereas neither Article 10 nor Recital 18 EHDS addresses whether the exercise

Downloaded from https://teseo.unitn.it/biolaw ISSN 2284-4503

silent on this question and falls squarely within the rules and specific safeguards that national legislators are required to lay down.[74]

5. The Opt-Out Right in the Secondary Use of Health Data

The EHDS establishes a structured regulatory framework for the secondary use of certain categories of electronic health data, aimed at facilitating their reuse for public interest purposes, scientific research, innovation, and public policymaking.[75] Under this framework, health data holders are required to make the relevant electronic health data available to the competent Health Data Access Body (HDAB), which may subsequently grant access to health data users through a data permit or an approved health data request.[76] As a counterpart to this data circulation model, the Regulation confers on natural persons an opt-out right enabling them to oppose the processing of their data for these secondary purposes.

Unlike the primary use regime, the secondary use opt-out is established in Article 71(1) as a full subjective right, directly conferred on citizens. It may be exercised at any time, is revocable, and requires no justification. Its rationale lies in the need to balance patient autonomy and informational self-determination with the technical viability of large-scale health research,[77] reconciling the imperative of comprehensive and representative datasets with the particularly sensitive character of personal electronic health data.[78]

The introduction of this right marks a significant departure from traditional models of health data governance: where the protection of individual autonomy in health data reuse has historically rested on informed consent, the EHDS governance architecture opts instead for an opt-out system, operating as an *ex post* mechanism of individual control, more compatible with the logic of continuous data circulation among multiple actors and purposes, and less prone to the practical limitations of prior consent in large-scale secondary use contexts.[79] The secondary use opt-out is also not fully assimilable to the GDPR right to object. Unlike the latter, it operates prospectively, preventing the data subjects' data from being in-

---

of the primary use opt-out is visible to them. The gap is therefore identified by comparison between the two provisions. Recital 18 EHDS does, however, provide that healthcare providers continue to document the treatment given and retain access to the data they have themselves recorded, so that data withheld from the interoperable services remain in the local record.

[74] Article 10(2) EHDS. On the institutional and technical-infrastructural, and not merely legal, dimensions of the changes the framework introduces, see P. TERZIS, O. E. SANTAMARIA ECHEVERRIA, *Interoperability and Governance in the European Health Data Space Regulation*, in *Medical Law International*, 23(4), 2023, 368-376.

[75] Articles 53 and 54 EHDS. See also Recital 61 EHDS.

[76] Articles 51, 53, 55, 57 and 60 EHDS, which respectively govern the minimum categories of electronic health data to be made available for secondary use, the permitted purposes of secondary use, the designation of Health Data Access Bodies, their tasks, and the obligation of health data holders to make the relevant data available to the competent Health Data Access Body upon request.

[77] M. KRUUS, *Opting Out of Scientific Research with Health Data*, cit. 165-189.

[78] Recital 54 EHDS.

[79] Relying solely on prior consent is neither sufficiently protective nor operationally practicable: P. TRIGO KRAMCSÁK, I. DE MIGUEL BERIAIN, *The Opt-Out Right for Secondary Uses of Personal Data in the European Health Data Space*, cit., 2 and 7. F. DE MONTALVO JÄÄSKELÄINEN, *Una reflexión desde la teoría de los derechos fundamentales*, cit. On the resulting shift from a consent-based approach to one grounded in the public interest, see E. SANTAMARÍA ECHEVERRÍA, *The European Health Data Space: A New Paradigm for Secondary Uses of Health Data for Scientific Research?*, in S. SLOKENBERGA, K. Ó CATHAOIR, M. SHABANI (eds.), *The European Health Data Space*, cit., 162-178.

Downloaded from https://teseo.unitn.it/biolaw ISSN 2284-4503

corporated into future access permits, without requiring justification or individual balancing. This strengthens the data subject's control but also delimits the right's scope, which cannot extend to authorizations already granted.

Once exercised, the opt-out prevents the data concerned from being made available under new access permits approved thereafter.[80] Article 71(3) second subparagraph expressly provides, however, that the right has no retroactive effect: it does not affect processing already authorised prior to its exercise.[81] The opt-out thus operates with essentially prospective efficacy, distinguishing it from the right to object and enabling a "preventive" exclusion of data from secondary use.[82]

The Regulation requires Member States to establish accessible and comprehensible opt-out mechanisms through which individuals may expressly communicate their wishes.[83] HDABs play a central role in the practical implementation of this right. Data subjects need not justify their decision and may reconsider their choice at any time, reinforcing individual control over health data.

5.1. Exceptions

The secondary use opt-out is likewise not absolute. Article 71(4) allows Member States to establish, in national law, exceptional mechanisms permitting access to data in respect of which the opt-out has been exercised, subject to a series of cumulative conditions. First, access must be requested by public entities or bodies entrusted with a public health mandate, or by entities acting on their behalf.[84] Second, the processing must serve specific enumerated purposes, including the protection of public health, public policymaking, the production of official statistics, or scientific research carried out for important reasons of public interest.[85] Third, it must be demonstrated that the data cannot be obtained by alternative means under equivalent conditions, and that the requirements applicable to data access permits are satisfied (Article 71(4)(b) and (c)). Any such exceptions must comply with principles of necessity and proportionality and incorporate specific safeguards for the protection of data subjects' fundamental rights, including the prohibition of re-identification.[86]

The HDAB must provide data in anonymized form where the data user's purpose can be adequately achieved using anonymized data. Access to pseudonymized data is available only where the data user

[80] Article 71(3), first subparagraph, EHDS, which prevents the data from being made available or otherwise processed under data permits issued under Article 68 or health data requests approved under Article 69 after the right has been exercised, where the data concerning that person can be identified in a dataset.

[81] According to the precept "The first subparagraph of this paragraph shall not affect the processing for secondary use of personal electronic health data relating to those natural persons pursuant to data permits or health data requests that were issued or approved before the natural persons exercised their right to opt out".

[82] P. Trigo Kramcsák, I. De Miguel Beriain, *The Opt-Out Right for Secondary Uses of Personal Data in the European Health Data Space*, cit.,9.

[83] Article 71 (2) EHDS.

[84] Article 71(4)(a) "The health data Access application or health data request is submitted by a public sector body or a Union institution, body, office or agency with a mandate to carry out tasks in the area of public health, or by another entity entrusted with carrying out public tasks in the area of public health, or acting on behalf of or commissioned by a public authority".

[85] Specifically, the provision states: "the purposes referred to in Article 53(1), points (a), (b) and (c) and scientific research for important reasons of public interest".

[86] Article 71(5) and (6) EHDS.

Downloaded from https://teseo.unitn.it/biolaw ISSN 2284-4503

demonstrates that anonymized data are insufficient for the purpose.[87] The possibility of introducing such exceptions may increase the regulatory fragmentation already present under the GDPR, owing to the wide margin of discretion conferred on Member States, and could generate significant divergences in the regulation of secondary use across national legal orders.[88] Member States are required to notify the Commission of the national provisions introducing these exceptional mechanisms,[89] reflecting the importance attached to European level oversight.

The right is subject to further limits. Under Article 71(8) EHDS, it does not apply where the data no longer permit the identification of the data subject, as in cases of full anonymization, nor does it require data holders to maintain, acquire or process additional information solely for the purpose of enabling its exercise. The right may also be displaced, under the conditions laid down in Article 71(4) EHDS, where access is requested for public health, public policy-making, official statistics, or scientific research carried out for important reasons of public interest. These limits confirm that the opt-out, while constituting a reinforced control instrument in the secondary use domain, does not operate outside the balancing of interests characteristic of European health data governance.[90]

Alongside these exceptions that modulate the opt-out's scope, the EHDS introduces an exception of greater structural significance, one capable of inverting the Regulation's general logic. While Member States are ordinarily prohibited from maintaining or introducing additional conditions for the processing of health data within the EHDS framework pursuant to Article 9(4) GDPR, certain categories of data are expressly excluded from this rule by virtue of Article 51(4) EHDS, which allows Member States to introduce stricter measures and additional safeguards at national level in order to protect the sensitivity and value of human genetic, epigenomic and genomic data, other human molecular data, data from wellness applications and health data from biobanks and associated databases, subject to notification to the Commission. Member States may accordingly establish additional safeguards for the secondary exchange of genetic data, including the possibility of requiring the data subject's explicit consent – an opt-in mechanism. A comparable logic governs the primary use domain: under Article 47(2) EHDS, interoperability between a wellness application and an EHR system does not entail the automatic exchange or transmission of the data it holds, such exchange being possible only in accordance with the user's wish-

[87] In such cases, the information required to reverse the pseudonymisation process shall remain exclusively under the control of the access body itself or, where applicable, of an entity acting as a trusted third party in accordance with the applicable national law. See R. RAK, *Anonymisation, Pseudonymisation and Secure Processing Environments Relating to the Secondary Use of Electronic Health Data in the European Health Data Space (EHDS)*, in *European Journal of Risk Regulation*, 15, 4, 2024, 928-939.

[88] D. CORTI, *Consenso (a fasi progressive), interesse pubblico per l'IA, opt-out per l'uso secondario: le nuove regole per la ricerca scientifica sui dati sanitari*, in *BioLaw Journal – Rivista di BioDiritto*, 1, 2025, 275-290.

[89] Article 71(7) EHDS.

[90] Articles 71(4) and 71(8) EHDS. Article 71(8) excludes the application of the right where the data no longer permit the identification of the data subject and clarifies that data holders are not required to maintain, acquire or process additional information solely to enable its exercise. Article 71(4), read together with Article 53(1)(a)–(c), permits access to data despite the exercise of the opt-out for specified public interest purposes. See also Article 11 GDPR.

Downloaded from https://teseo.unitn.it/biolaw ISSN 2284-4503

es, and Recital 50 leaves Member States free to regulate other aspects of the use of wellness applications.[91]

The literature has identified this as a manifestation of "genetic exceptionalism": the tendency to subject genetic data to a singular legal regime in view of their particular sensitivity, hereditary character, and the risks their processing may pose not only to the individual but also to relatives and communities.[92] This exception has attracted well-founded scholarly criticism. From a scientific perspective, an *opt-in* mechanism may seriously compromise the representativeness and comprehensiveness of datasets. Empirical studies demonstrate statistically significant differences in participation rates: *opt-out* procedures may achieve rates as high as 95.6%, while *opt-in* rates may fall to 21%.[93] *Opt-in* studies also tend to under-represent individuals with vulnerable conditions, a particular concern for rare diseases, the overwhelming majority of which have a genetic basis.[94] The European Society of Human Genetics (ESHG) has expressly stated that an *opt-in* mechanism for genetic data is not only arbitrary but may risk significantly obstructing progress in human genetics in Europe.[95]

From a legal perspective, introducing an *opt-in* mechanism does not necessarily entail that consent becomes the legal basis for data processing. Individual control over data exists on a spectrum that cannot be reduced to the *opt-in/opt-out* dichotomy:[96] A Member State could establish an *opt-in* mechanism for genomic data while maintaining legal obligation or public interest as the legal basis, or alternatively reinforce individual control through a differentiated *opt-out* mechanism for this category of data without altering the legal basis or transitioning to prior consent.[97] In any event, the prospect of heterogeneous national solutions creates a systemic risk of regulatory fragmentation capable of reproducing, and even

[91] Article 51(4) EHDS, read together with Article 51(1), points (f), (g), (i) and (q). Recital 52 EHDS states that Member States may no longer maintain or introduce, under Article 9(4) GDPR, additional conditions – including limitations and specific provisions requiring the consent of natural persons – in relation to processing for the secondary use of personal electronic health data under the Regulation, save for the stricter measures and additional safeguards it itself provides for. On the primary use side, see Article 47(2) and Recital 50 EHDS. See also K. O'CATHAOIR, *The EHDS and Electronic Health Records. GDPR+ or Transforming Patients' Rights?*, in S. SLOKENBERGA, K. O'CATHAOIR, M. SHABANI (eds.), *The European Health Data Space. Examining a New Era in Data Protection*, Abingdon-New York, 2025, 26-27.

[92] G. LAZCOZ, G. COMANDÉ, *Genetic Data Sharing in the European Health Data Space: An Urgent Call for Coordinated Action by the Member States*, in *BioLaw Journal – Rivista di BioDiritto*, 1, 2026, 166-167. On the interplay between genomic data, consent and data altruism in this context, see E. EL ASRY, J. MANSNÉRUS, S. LIEDE, *Striking the Balance: Genomic Data, Consent and Altruism in the European Health Data Space*, in S. Slokenberga, K. Ó Cathaoir, M. Shabani (eds.), *The European Health Data Space. Examining a New Era in Data Protection*, Abingdon-New York, 2025, 110-135.

[93] J. G. BERRY, P. RYAN, M. S. GOLD, A. J. BRAUNACK-MAYER, K. M. DUSZYNSKI, *A Randomised Controlled Trial to Compare Opt-In and Opt-Out Parental Consent for Childhood Vaccine Safety Surveillance Using Data Linkage*, in *Journal of Medical Ethics*, 38, 10, 2012, 619-625; M. HERMUS, C. H. SCHARLOO-KARELS, M. A. IKRAM *et al.*, *Opt-In versus Opt-Out for the Secondary Use of Routinely Recorded Health Data: A Randomized Controlled Trial*, in *European Journal of Internal Medicine*, 133, 2025, 100-105.

[94] Y. DE MAN, Y. WIELAND-JORNA, B. TORENSMA *et al.*, *Opt-In and Opt-Out Consent Procedures for the Reuse of Routinely Recorded Health Data in Scientific Research and Their Consequences for Consent Rate and Consent Bias: Systematic Review*, in *Journal of Medical Internet Research*, 25, 2023.

[95] European Society of Human Genetics (ESHG), *Opting-in to data sharing in the European Health Data Space will disadvantage research on personalised medicine*. https://www.eshg.org (last accessed: 26 May 2026)

[96] G. LAZCOZ, G. COMANDÉ, *Genetic Data Sharing in the European Health Data Space*, cit.,172-173.

[97] G. LAZCOZ, G. COMANDÉ, *Genetic Data Sharing in the European Health Data Space*, cit.,173-174.

Downloaded from https://teseo.unitn.it/biolaw ISSN 2284-4503

aggravating, the asymmetries already generated by the uneven application of Article 9(4) GDPR across national legal orders.[98]

5.2. Implementation Challenges

Implementation is not a question for the future. Chapter IV, which governs the secondary use of health data, does not apply until 26 March 2029. For certain categories of electronic health data, including human genetic, epigenomic and genomic data, the application of Chapter IV is deferred until 26 March 2031 (Article 105 EHDS). That long lead time is precisely why the question matters now: Member States are designing the mechanism at this moment, and the choices they make over the next few years will determine what the right actually amounts to. TEHDAS2 recognized as much when it issued a dedicated guideline for health data access bodies in September 2025, intended to align national structures around a common approach.[99] The very fact that such an instrument was considered necessary demonstrates that fragmentation is not merely a hypothetical concern but a present one.

The first set of challenges concerns national governance. Article 71(2) requires only that the opt-out mechanism be accessible and easy to understand; it says nothing about how it should be designed. That silence leaves a wide range of institutional options, and the choice between them matters. The most basic question is where the right is exercised: through a single national portal, through the health data access body, through data holders, or through some combination of these.[100] The Regulation does, however, provide one point of reference. Article 58(2) places the duty to inform individuals about the opt-out procedure and to facilitate its exercise on the competent access body, so that the system is, in its basic design, access-body-centered.[101] What remains open is everything that gives that design practical shape. A centralized system means that individuals declare their wish once and that the declaration then travels reliably to every national database, which the national experts interviewed in a recent twenty-three-country study identified as essential.[102] A decentralized system may be easier to reach for people with limited digital skills, but it creates more points of failure and places a heavier administrative load on the health system.

There is a further problem for States with devolved health competences. Article 55(2) allows a Member State to designate more than one access body, requiring only that one of them be given a coordinating role; beyond that, the Regulation says nothing about how those bodies should relate to one another, and it falls to the national legislature to ensure that an opt-out is applied consistently across all of them and by every data holder.[103] Spain illustrates this difficulty well. Its emerging model combines a federated structure, in which the Autonomous Communities retain sovereignty over the data held in their territories, with a centralized strategy in which the national access function sits with the Ministry of Health; yet progress across regions in establishing data governance bodies and infrastructures remains markedly

[98] DG Sante, *Assessment of the EU Member States' Rules on Health Data in the Light of GDPR*, cit.

[99] TEHDAS2, *M8.1 Draft Guideline to Health Data Access Bodies "How to implement opt-out from secondary use of electronic health data"*, 7 September 2025, www.tehdas.eu (last visited 11/08/2026).

[100] TEHDAS2, *M8.1 Draft Guideline*, cit., 20 ff.

[101] Article 58(2) EHDS. On the access-body-centred character of the system, see P. Trigo Kramcsák, I. De Miguel Beriain, *The Opt-Out Right for Secondary Uses of Personal Data in the European Health Data Space*, cit.,8.

[102] P. Cervera de la Cruz, T. Lalova-Spinks, M. Shabani, *op.cit.*

[103] Article 55(2) EHDS. See also TEHDAS2, *M8.1 Draft Guideline*, cit., 21.

Downloaded from https://teseo.unitn.it/biolaw ISSN 2284-4503

uneven, and the national legislation implementing the Regulation is still being prepared.[104] The point is not particular to one State. Wherever health competences are devolved, the consistency of the opt-out depends on coordination that the Regulation does not itself provide. Institutional design is only as good as the technical infrastructure that carries it out. In practice, the right depends on an opt-out register, and that register has to satisfy two demands that pull against each other. It must be robust enough to keep the data out, which requires filtering at two points: at source, by the data holder, and again when a dataset is assembled for a permit.[105] At the same time, the register is itself a processing operation on especially sensitive data, since it records a choice from which unwanted inferences can be drawn; data minimization and purpose limitation therefore apply with particular force.[106] The paradox is plain: an instrument designed to protect informational self-determination creates a privacy risk of its own.

The second question of substance for national legislatures is granularity. The Regulation does not expressly provide for a selective opt-out, and Article 71(3) has accordingly been read as categorical in its terms, establishing a logic of general exclusion that operates at the level of the individual rather than in relation to discrete elements of their electronic health data.[107] Some national analyses already proceed on the assumption that the right is binary, an all-or-nothing choice between full availability and full exclusion.[108] That reading does not, however, foreclose implementing mechanisms that introduce a degree of granularity in practice, and it is at national level that the question will in fact be resolved. The choice goes to the heart of the balance the mechanism is meant to strike. An all-or-nothing model is easier to run and keeps the system from sliding into a consent logic, which would cut against the rationale of the EHDS, but it may push people into blanket exclusion when their objection was to one use only. A granular model gives individuals finer control at the cost of organizational complexity, makes datasets harder to compare across Member States, and risks confusing people or wearing down their willingness to decide at all.[109] The emerging view favors a middle path: a small number of meaningful levels, two or three, tracking real differences in sensitivity and public expectation without exceeding what individuals can reasonably be asked to understand or what systems can be built to deliver.[110] Which levels count as essential, however, will vary with legal tradition and cultural expectation, so even the middle path does not remove the risk of fragmentation.

These are not merely organizational choices. They determine how much autonomy the right actually confers. A mechanism that is too rigid reduces the opt-out to a formality, forcing people to choose between full participation in secondary use and total withdrawal even when their objection is limited to particular purposes or particular kinds of data. A mechanism that is too elaborate makes the right hard-

[104] Fundación Instituto Roche, *El Espacio Europeo de Datos de Salud y su implementación en España*, Madrid, 2026, 45-46 and 51. On the challenges of ensuring appropriate safeguards where health data are shared through federated structures, see M. Kogut-Czarkowska, M. Shabani, *Federated Networks and Secondary Uses of Health Data*, in S. Slokenberga, K. Ó Cathaoir, M. Shabani (eds.), *The European Health Data Space. Examining a New Era in Data Protection*, Abingdon-New York, 2025, 229-254.

[105] TEHDAS2, *M8.1 Draft Guideline*, cit., 23 ff.

[106] TEHDAS2, *M8.1 Draft Guideline*, cit., 23. See also Articles 5(1)(b) and (c) GDPR.

[107] P. Trigo Kramcsák, I. De Miguel Beriain, *The Opt-Out Right for Secondary Uses of Personal Data in the European Health Data Space*, cit.,9.

[108] Fundación Instituto Roche, cit., 39.

[109] TEHDAS2, *M8.1 Draft Guideline*, cit., 19 ff.; P. Cervera de la Cruz, T. Lalova-Spinks, M. Shabani, op. cit.

[110] TEHDAS2, *M8.1 Draft Guideline*, cit., 20.

Downloaded from https://teseo.unitn.it/biolaw ISSN 2284-4503

er to exercise and imposes a decisional burden difficult to square with the accessibility and comprehensibility Article 71(2) demands. Autonomy is not secured, then, by recognizing the right in the abstract. It is secured, or lost, in the way national law sets the conditions for exercising it. The Regulation confers the entitlement; national implementation determines what it is worth.

Fragmentation, moreover, operates along a second axis that is easily overlooked. Member States are asked to design not only the modalities of the right but also the mechanism by which it can be set aside. Article 71(4) leaves the override to national law, and the conditions it lays down are framed in terms open to appreciable interpretative variation.[111] The initiative to invoke the exception lies with the health data user rather than with the authority, and the burden of demonstrating the required grounds falls on the applicant; but it is the access body that decides, case by case, whether those grounds hold.[112] Two of the operative concepts are notoriously unsettled. What counts as an important reason of public interest has never attracted a common European understanding, and national supervisory practice under the GDPR has ranged from the generous to the restrictive.[113] The notion of scientific research is equally elastic, and Recital 61 invites a broad reading that extends to technological development and privately funded work, which sits uneasily with the narrower conception that data protection authorities have defended.[114] Nor is the frame stable: the Digital Omnibus proposal published in November 2025 would insert a broad statutory definition of scientific research into the GDPR itself, with consequences for how the EHDS override is read.[115] The upshot is that Member States may diverge not only in how easily the right can be exercised but in how easily it can be overcome. Article 71(7) requires them to notify the Commission of the national measures adopted, which supplies transparency but no substantive alignment.[116]

A third question, less discussed, concerns the boundary of the right itself. Article 71(8) provides that a data holder need not maintain, acquire or process additional information in order to identify a data subject for the sole purpose of complying with the opt-out, mirroring the logic of Article 11 GDPR.[117] The

[111] Article 71(4) EHDS and Recital 54.

[112] P. TRIGO KRAMCSÁK, I. DE MIGUEL BERIAIN, *The Opt-Out Right for Secondary Uses of Personal Data in the European Health Data Space*, cit.,11-12.

[113] M. KRUUS, *Opting Out of Scientific Research with Health Data*, cit. P. QUINN, *Research under the GDPR – A Level Playing Field for Public and Private Sector Research?*, in *Life Sciences, Society and Policy*, 17, 1, 2021, 4. On the indeterminacy of the public interest standard and the discretion it leaves to health data access bodies, see T. PETROČNIK, *Secondary Use of Health Data in the EHDS: Public Interest and the Role of HDABs*, in S. SLOKENBERGA, K. Ó CATHAOIR, M. SHABANI (eds.), *The European Health Data Space*, cit., 181-206. See also J. REICHEL, *Administrative Tools for Balancing Societal and Individual Interests – Data Protection Safeguards and Administrative Procedural Guarantees in Secondary Use in the European Health Data Space*, in S. Slokenberga, K. Ó Cathaoir, M. Shabani (eds.), *The European Health Data Space. Examining a New Era in Data Protection*, Abingdon-New York, 2025, 207-228.

[114] Recital 61 EHDS. On the tension with the narrower reading defended by data protection authorities, see P. QUINN, E. ELLYNE, C. YAO, *Will the GDPR Restrain Health Data Access Bodies under the European Health Data Space (EHDS)?*, in *Computer Law & Security Review*, 54, 2024.

[115] European Commission, *Proposal for a Regulation amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework (Digital Omnibus)*, COM(2025) 837 final, 19 November 2025, Recital 29 and proposed Article 4(38) GDPR.

[116] Article 71(7) EHDS.

[117] Article 71(8) EHDS; cf. Article 11 GDPR.

Downloaded from https://teseo.unitn.it/biolaw ISSN 2284-4503

right therefore reaches only as far as identifiability does, and identifiability is not a fixed property of a dataset. In its 2025 judgment in *EDPS v Single Resolution Board* the Court of Justice confirmed a relative and contextual approach, under which whether pseudonymized information remains personal depends on the means reasonably likely to be used by the particular actor holding it.[118] The consequence for implementation is direct: the scope of the opt-out cannot be settled in the abstract but must be assessed against the technical and organizational realities of each actor along the chain, and Member States designing filtering rules will have to decide, in practice, at which points in that chain the right bites.[119]

The same design pressures bear on reversibility, which is harder to deliver for secondary use than for primary use. The difficulty is sharpest where data have already been drawn into an ongoing analysis: withdrawing them mid-course would undermine the integrity of the results and make the analysis impossible to verify. That is precisely why Article 71(3), second subparagraph, gives the right prospective effect only. It also means that access bodies need systems able to reconstruct the state of the register as it stood on the day any given permit was issued, since that is what determines which data were properly included.[120] One further consequence is easily missed. Article 66 requires access bodies to supply data in anonymized form wherever that suffices, yet anonymization is itself a processing operation performed on identifiable data, so an opt-out blocks not just the use of the data but the whole preparatory chain, anonymized statistical outputs included.[121] From a strict data protection standpoint that result is hard to explain, since anonymized data fall outside the scope of the GDPR altogether; it is intelligible only if the opt-out is understood to protect a broader conception of informational control than the one the GDPR ordinarily secures.[122] The right reaches further than a quick reading of Article 71 would suggest, and the reason it does so is itself revealing.

None of this matters, though, if the premise behind the system is forgotten. The opt-out is not what justifies secondary use; the justification lies in the public benefit secondary use produces. The opt-out is a safety valve, meant to be a last resort.[123] Its success therefore cannot be measured by accessibility alone, since a system in which opting out became the norm would defeat the object of the Regulation. What evidence there is suggests that opt-out rates turn less on technical design than on institutional trust and on how the issue is reported. Finland is the clearest illustration. Despite a long tradition of secondary use and unusually high confidence in public institutions, press coverage of the EHDS in 2024 produced a surge of requests to Findata large enough to disrupt its ordinary services.[124] In the Nether-

[118] CJEU, judgment of 4 September 2025, C-413/23 P, *European Data Protection Supervisor v Single Resolution Board*, ECLI:EU:C:2025:645.

[119] P. TRIGO KRAMCSÁK, I. DE MIGUEL BERIAIN, *The Opt-Out Right for Secondary Uses of Personal Data in the European Health Data Space*, cit.,14.

[120] TEHDAS2, *M8.1 Draft Guideline*, cit., 27.

[121] Articles 66 and 71(3) EHDS; TEHDAS2, *M8.1 Draft Guideline*, cit., 18. On anonymization as a processing operation, see Article 4(2) and Recital 26 GDPR.

[122] P. TRIGO KRAMCSÁK, I. DE MIGUEL BERIAIN, *The Opt-Out Right for Secondary Uses of Personal Data in the European Health Data Space*, cit.,13.

[123] TEHDAS2, *M8.1 Draft Guideline*, cit., 14.

[124] Findata, *Delays in Findata's Services due to a High Number of Citizens' GDPR Requests*, 2024; P. CERVERA DE LA CRUZ, T. LALOVA-SPINKS, M. SHABANI, op. cit. On the absence of an express opt-out right under the Finnish *Act on the Secondary Use of Health and Social Data (552/2019)* and the low number of objections recorded up to 2024, see M. SALOKANNEL, *Opting-in or -out or Not at All*, cit.

Downloaded from https://teseo.unitn.it/biolaw ISSN 2284-4503

lands, meanwhile, the Regulation has been characterized in some quarters as handing the health system over to large technology companies.[125] High-trust environments, in other words, are not immune. National authorities are alive to the risk: recent Spanish analysis identifies the combination of low data literacy and misinformation as capable of producing opt-out on a mass scale, and recommends public information campaigns precisely in order to forestall it.[126]

Communication is therefore central, and it is not merely a matter of policy. Since the EHDS builds upon the GDPR rather than displacing it, the transparency obligations of Articles 13 and 14 GDPR continue to apply. Article 14 carries most of the weight in this setting, because individuals will ordinarily have no direct relationship with the access bodies or data users handling their records, which makes information provided in the absence of direct collection the principal channel through which they can learn that the right exists at all.[127] The obligation, however, must be pitched carefully. Too little information hollows the right out, since there is no real opt-out if people do not know it exists, while too much, or the wrong kind, can cause alarm and trigger exclusions on a scale that damages the system.[128] Health professionals are the actors the public trusts most and are the obvious messengers, but giving them the role carries a risk: patients may read it as the clinical relationship being used to serve secondary purposes, which would erode the confidentiality that relationship rests on.[129] Article 84 provides a legal basis for work on digital health literacy, but it is drafted in programmatic terms and leaves the substance of any communication strategy to Member States. Where information arrives late, in inaccessible form, or not at all, the right is neutralized before it can be exercised.

One further point has attracted little attention: an opt-out does not travel. It takes effect only for data generated and held in the State where it is made, so anyone who has lived or been treated in more than one Member State would have to opt out again in each.[130] This follows logically enough from leaving the mechanism to national law, but it sits awkwardly with the idea of a European data space and with the accessibility Article 71(2) demands. It is probably the point at which coordination between Member States is most urgently needed.

That these difficulties are real rather than speculative is confirmed by the Member States themselves. During the adoption procedure Estonia recorded its concern that an obligatory opt-out could erode the quality and completeness of the datasets research depends on, while Finland and Denmark, both of

[125] P. Cervera de la Cruz, T. Lalova-Spinks, M. Shabani, *op. cit*.

[126] Fundación Instituto Roche, cit., 50 and 52.

[127] Recital 8 EHDS; Articles 13 and 14 GDPR. See P. Trigo Kramcsák, I. De Miguel Beriain, *The Opt-Out Right for Secondary Uses of Personal Data in the European Health Data Space*, cit.,15.

[128] P. Cervera de la Cruz, T. Lalova-Spinks, M. Shabani, op. cit. M. Saelaert, L. Mathieu, W. Van Hoof, B. Devleesschauwer, *Expanding citizen engagement in the secondary use of health data: an opportunity for national health data access bodies to realise the intentions of the European Health Data Space*, in *Archives of Public Health*, 81, 2023, 168. On the risk of systematic exclusion driven by lack of awareness rather than genuinely informed choice, see S. van Drumpt *et al.*, *Secondary use under the European Health Data Space: setting the scene and towards a research agenda on privacy-enhancing technologies*, in *Frontiers in Digital Health*, 7, 2025, 1602101.

[129] P. Cervera de la Cruz, T. Lalova-Spinks, M. Shabani, op. cit. Standing Committee of European Doctors (CPME), *Position on the European Health Data Space*, Brussels, 2022. See also Recital 24 EHDS.

[130] TEHDAS2, *M8.1 Draft Guideline*, cit., 20.

Downloaded from https://teseo.unitn.it/biolaw ISSN 2284-4503

which voted against the text, warned that implementation would be technically difficult.[131] The challenge is not simply to build a legally sound mechanism. It is to build enough trust that the opt-out remains what it was designed to be: an exceptional safeguard, rather than the default answer to uncertainty. In the end the right will succeed or fail not on the strength of its recognition in the Regulation but on whether Member States can design governance models that are technically workable, sufficiently aligned with one another, and capable of holding together individual autonomy, public confidence and the social value of secondary use.

6. Synthesis Table of the Primary and Secondary Opt-Out Regimes

The preceding analysis has demonstrated that the opt-out right does not constitute a uniform legal institution within the EHDS. Its dual configuration reflects legislative choices regarding the balance between individual autonomy and the collective interest that go beyond purely formal distinctions. The following table summarizes the principal differences between the two regimes.

	Primary use of data	Secondary use of data
Purpose	Direct healthcare provision; diagnosis, treatment, continuity of care	Scientific research, innovation, public health, and health policymaking
Nature of the right	Optional, dependent upon recognition under national law	Fully-fledged subjective right directly conferred by the Regulation
Legal base	Article 10	Article 71
Scope	Restriction of access to data through interoperable services (without excluding registration within the EHR)	Exclusion of data processing for secondary use in future access requests or disclosures
Exercise of the right	Configured by each Member State (conditions, procedures, and safeguards)	Directly exercisable, at any time and without justification
Reversibility	Yes, through revocation of the restriction	Yes, through withdrawal of the opt-out (without retroactive effects)
Exceptions	Access permitted in situations involving vital interests (Article 9(2)(c) GDPR)	Exceptions based on public interest (public health, research) subject to strict conditions (Article 71(4))
Effects	Conditional limitation: does not prevent access in critical or emergency healthcare situations	Prospective effect: prevents future processing but does not affect previously authorized processing

[131] Council of the European Union, *Draft Regulation of the European Parliament and of the Council on the European Health Data Space — Adoption of the legislative act — Statements*, Brussels, 2025. See also P. CERVERA DE LA CRUZ, T. LALOVA-SPINKS, M. SHABANI, *op. cit.*

Downloaded from https://teseo.unitn.it/biolaw ISSN 2284-4503

Extent of the right	Limited to restricting access to data, without preventing their use in healthcare provision	Enables exclusion of data from secondary use purposes, subject to the exceptions provided for by the Regulation
Protected interest	Primacy of continuity of care and patient safety	Balance between informational self-determination and the social value of health data for scientific advancement

**Table compiled by the author*

The comparison reveals a structural asymmetry. In the primary use domain, the prevailing logic is the protection of the healthcare system's functionality. In the secondary use domain, greater recognition is afforded to individual autonomy, albeit conditioned by the need to preserve the social value of data. This divergence underscores the difficulty of constructing a coherent model that reconciles the use of health data with the protection of fundamental rights. The broad discretion granted to Member States introduces a clear risk of regulatory fragmentation, affecting both the effectiveness of the right and the coherence of the EHDS itself.[132] Differences in the configuration of the primary use opt-out and in the articulation of secondary use exceptions may produce unequal levels of protection across national legal orders.[133] The opt-out right emerges as a central element of the EHDS data governance model, but its effectiveness depends on the rigour of practical implementation, the adequacy of information provided to citizens, and the application of the principles of necessity and proportionality when exceptions are invoked.

7. Conclusions

The opt-out right in the EHDS is not a uniform right. Its scope, nature, and effects vary significantly between the primary and secondary use domains, reflecting different balances of interests. This duality, as argued throughout this paper, is not merely technical: it expresses legislative policy choices with direct implications for fundamental rights, including the rights to the protection of personal data and to privacy.

In the primary use domain, the opt-out is limited and conditional. Its discretionary nature – dependent on its incorporation by the Member States – together with the primacy of healthcare purpose, significantly restricts effective patient control. The right does not permit the complete exclusion of data from the system; it restricts interoperable accessibility only, while clinical documentation obligations and professional access in care settings remain intact.

In the secondary use domain, the opt-out is a genuine subjective right, exercised at any time without justification. Its principal effect is to prevent future processing of data for reuse purposes, meaningfully reinforcing the data subject's informational self-determination. Yet it is equally not absolute: it is modu-

[132] L. MARKSCHIES, *The European Health Data Space: The Next Step in Data Regulation*, cit. 425-440.

[133] X. YAO *et al.*, *Balancing Scientific and Commercial Interests: The European Health Data Space Response to Commercial Scientific Research*, in *INQUIRY: The Journal of Health Care Organization, Provision, and Financing*, 63, 2026.

Downloaded from https://teseo.unitn.it/biolaw ISSN 2284-4503

lated by public interest exceptions and lacks retroactive effect with respect to previously authorised processing.

The comparison reveals a structural asymmetry that underscores the difficulty of reconciling the exploitation of health data with the protection of fundamental rights. The broad discretion conferred on Member States introduces an evident risk of regulatory fragmentation that may compromise both the effectiveness of the right and the coherence of the EHDS.[134] In particular, differences in the configuration of the primary use opt-out, and the possibility that Member States introduce an *opt-in* mechanism for genetic data, may generate differing levels of protection across national legal orders that are difficult to reconcile with the Regulation's harmonizing rationale.[135]

The model designed by the EHDS reflects a tension between maximizing the social value of health data, and protecting individual autonomy. In response to the limitations of traditional consent, the opt-out right emerges as a balancing instrument. Its scope, determined by the Regulation and concretized by each Member State with possible exceptions, articulates a balance between individual autonomy and the general interest in line with the Declaration of Helsinki and the Oviedo Convention. The practical functioning of the system will depend on the case-by-case application of necessity and proportionality, particularly in scientific research, where the justification for the inability to resort to alternative data sources may vary considerably depending on context.[136] Uncertainties also persist regarding the practical organization of the opt-out procedure and the entities responsible for managing it, issues that the Regulation leaves to national determination and that risk producing heterogeneous outcomes.[137]

Ultimately, the success of the EHDS opt-out regime will depend not only on its legal design but also on the extent to which its implementation across the Member States is capable of ensuring a consistent level of protection for individuals while preserving the public interest objectives that underpin the Regulation.

[134] L. MARKSCHIES, *The European Health Data Space: The Next Step in Data Regulation*, cit., 425-440.

[135] X. YAO *et al.*, *Balancing Scientific and Commercial Interests*, cit.

[136] Comité de Bioética de España, *Informe sobre la supervisión ética del tratamiento de datos en el contexto del Espacio Europeo de Datos de Salud (EEDS)*, Madrid, 2025.

[137] V.L. RAPOSO, *Can Personal Data Be Recycled? The Reuse and Repurposing of Data under the EHDS*, in *International Journal of Law and Information Technology*, 33, 2025.

Downloaded from https://teseo.unitn.it/biolaw ISSN 2284-4503