

The European Health Data Space (EHDS)**

The European Health Data Space (EHDS) regulation was accepted on 11 February 2025, the full applicability will be achieved from 26 March 2031. The Regulation has double aims, firstly to improve the patients' access to and control over their personal electronic health data in the context of healthcare and secondly to better achieve other purposes that would benefit society, such as to support research, patient safety, personalised medicine, health threats (including pandemics), innovation, policymaking, official statistics or regulatory activities. The EHDS is the first EU common dataspace with many promises, expectations and challenges.

Keywords: *European Health Data Space, EHDS, health data, data law.*

1. Introduction

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 (EHDS Regulation) aims to optimise the exchange of and access to health information within the EU.

The European Health Data Space (EHDS) represents the first common EU data space initiative as part of the broader European data strategy aiming to meet the needs of a data-driven economy. The goal is to promote the secure and trustworthy use and sharing of data across 14 key sectors, including agriculture, energy, transport, and finance. According to the official announcement „*The EU will become an attractive, secure and dynamic data economy by setting clear and fair rules on access*

* Vice President of International Affairs, National Authority for Data Protection and Freedom of Information (Naih).

** The paper is the text of a keynote speech presented at the 33rd European Conference of Personal Data Protection Authorities (“Spring Conference”), hosted by the Personal Data Protection Service and held in Batumi. The information and views set out in this article are those of the author and do not necessarily reflect the official opinion of the European Commission.

and re-use of data; investing in next generation tools and infrastructures to store and process data; joining forces in European cloud capacity; pooling European data in key sectors, with common and interoperable data spaces and giving users rights, tools and skills to stay in full control of their data.”¹

The (re)use of personal data stored by public sector entities is only allowed under strict guarantees under EU data laws, which all follow an "access-based" approach, exemplified by horizontal regulations such as the Data Governance Act (DGA), Data Act (DA), and the Public Sector Information Directive (PSI). Anonymization is the general rule, and reidentification is explicitly prohibited by law. Furthermore, new rules have been introduced concerning non-personal data and the protection of the interests of legal persons. Neutral data intermediation services under the DGA aim to facilitate commercial relationships between data subjects, data holders, and users (for-profit). In parallel, altruistic data-sharing organizations, operating on a cost-recovery and nonprofit basis, support the voluntary, free-of-charge sharing of personal and non-personal data for public interest purposes. However, respecting the already existing horizontal EU legislation the EHDS introduces new sector-specific and *lex specialis* rules.

2. Dual Objectives of EHDS

1. Primary Data Use: Patients will have reinforced data protection rights in particular the right to access, to data portability, and to control over their personal electronic health data.

This includes:

- Adding personal health information;
- Restricting access to specific parts or individuals;
- Viewing access history;
- Requesting corrections in case of errors;
- Accessing their health data in a standardized European format.

2. Secondary Data Use: Electronic health data may also be used for broader societal goals such as:

- Research and innovation;
- Policy-making;
- Public health preparedness and response (including pandemics);
- Official statistics;
- Regulatory activities;
- Patient safety;
- Personalized medicine.

¹ European Commission, European Data Strategy, Making the EU a Role Model for a Society Empowered by Data, <commission.europa.eu/strategy-and-policy/priorities-2019-2024> [25.06.2025].

3. Implementation Timelines

2027:

- Member States must establish digital health and health access authorities and national contact points.

2029:

- Key EHDS services must be operational.
- Patients must have access to the first three data categories (medical history, e-prescriptions, e-dispensation).
- EHR systems must comply with EHDS specifications.
- Data users can submit applications for certain categories.
- Data holders must submit dataset descriptions to the access-granting authority.

2031:

- All EHDS services must be fully operational.
- Patients must have access to all their data.
- Marketed EHR systems must comply with EHDS specifications across all categories.
- Data users can apply for all data categories.
- Data holders must provide dataset descriptions.

4. Third countries

According to Preamble 35, the EHDS also supports exchanges of personal electronic health data with national contact points for digital health of relevant third countries and systems established at international level by international organisations in order to contribute to the continuity of healthcare. This is particularly relevant for individuals travelling to and from neighbouring third countries, candidate countries, and the associated overseas countries and territories. The connection of such national contact points for digital health of third countries to MyHealth@EU and the interoperability with digital systems established at international level by international organisations should be subject to a compliance check of the European Commission ensuring the compliance of those contact points and digital systems with the technical specifications, data protection rules and other requirements of MyHealth@EU. In addition, given that the connection to MyHealth@EU will entail transfers of personal electronic health data to third countries, such as sharing a patient summary when the patient seeks care in that third country, relevant transfer instruments under Chapter V of Regulation (EU) 2016/679 should be put in place. The Commission should be empowered to adopt implementing acts to facilitate the connection of such national contact points for digital health of third countries and systems established at international level by international organisations to MyHealth@EU. When preparing

those implementing acts, the Commission should take into account Member States' national security interests.

For secondary use, following assessment and joining HealthData@EU, access is only available from 2035 onward.

5. Data Categories and Sources

From the healthcare system:

- Admission documents, medical records, referrals;
- Biological samples, imaging, sensory and metadata;
- Prescriptions, predictive/personalized medicine data;
- Monitoring and control data.

From researchers and industry:

- Aggregated database analyses;
- Exploratory datasets;
- Case studies, biological sample analysis.

6. Opt-Out Rights

Except where vital interests must be protected, Member States may allow patients to opt out of data access:

- By healthcare professionals (primary use);
- Or further reuse (secondary use).

However, public interest use, policy-making, statistical, and research access are excluded from opt-out options.

7. Prohibited Secondary Uses

According to Article 54 of the EHDS regulation health data users may only process data in line with the purposes authorized in the:

- Data permit under Article 68;
- Approved data application under Article 69;
- Specific cases under Article 67(3) or approval under Article 75.

It is forbidden to use the data for:

- Making disadvantageous decisions based on electronic health data (e.g., with legal, economic, or social impacts);
- Employment or service-related discrimination (e.g., insurance, credit exclusions);
- Advertising or marketing;
- Developing harmful or addictive products (e.g., drugs, alcohol, tobacco, weapons);

- Activities violating ethical norms defined by national laws.

8. Governance Structure of the EHDS

Infrastructure includes:

- The already existing MyHealth@EU and HealthData@EU infrastructures;
- National contact points;
- Digital health authorities;
- Data access-granting bodies (to authorize access, to supervise compliance, to impose sanctions, biannual reporting);
- Market surveillance authorities (to supervise electronic health record systems);
- The EHDS Board (shall be composed of two representatives per Member State, namely one representative for primary use purposes and one for secondary use purposes, nominated by each Member State; each Member State shall have one vote)
- Data holders and users.

9. Data Protection and Processing Principles Apply

The purpose of data processing standards is to protect fundamental human rights, not to alter or hinder sector-specific legal or professional practices. Processing must meet the standards of necessity and proportionality. The objective must justify the intrusion into privacy; "more effective medication" does not justify "more invasive development methods."

- Risk-based approach: Protection levels must correspond to the risks to individuals.
- Compliance: If the main process is non-compliant, the data processing cannot be compliant.
- Primary processing typically involves personal and identifiable data.
- Secondary processing requires access approval and typically involves anonymized or pseudonymized data.
- Anonymization is considered processing (requiring a legal basis), but once completed, the data is no longer considered personal data and falls outside the GDPR's scope.

Data protection authorities must be informed about imposed sanctions of the health data authorities and issues related to secondary data processing, and they should share relevant information to ensure rule enforcement.

10. Conclusion

The EHDS enables individuals to access, control, and share their electronic health data across borders, improving healthcare safety and patients' comfort. It also allows for the secure reuse of health data in research, innovation, policymaking, and regulatory activities. According to the European Commission, this could save up to €11 billion² in the EU over the next decade. Additionally, the EHDS supports the development of a single market for secure electronic health record systems that serve both primary and secondary uses.

On the other hand, due to its complexity and size the new infrastructures significantly raise the level of data protection risks in the form of various threats, including cyberattacks, insider threats, and data breaches. All these threats and injuries can lead to unauthorized access, loss of control, and great potential harm to individuals. These risks are further complicated by the sensitive nature of health data.

Bibliography:

1. European Commission, European Data Strategy, Making the EU a Role Model for a Society Empowered by Data, <commission.europa.eu/strategy-and-policy/priorities-2019-2024> [25.06.2025].
2. European Commission, Questions and answers - EU Health: European Health Data Space (EHDS), <ec.europa.eu/commission/presscorner> [25.06.2025].

² European Commission, Questions and answers - EU Health: European Health Data Space (EHDS), <ec.europa.eu/commission/presscorner> [25.06.2025].