EPF's analysis of the European Health Data Space Regulation

February 2025

This analysis aims to inform the EPF's membership about the most relevant changes and obligations introduced by the European Health Data Space (EHDS) regulation. For more detailed information, refer to the official text of the regulation, and please note that several provisions will be detailed in the implementing acts, which will provide further clarification on technical standards, requirements, and specifications. The current version of the regulation is available here.

1. Introduction

On 3rd May 2022, the European Commission proposed a regulation to establish the European Health Data Space (EHDS)[1], the first of nine sector-specific data spaces envisioned in the 2020 *European strategy for data*[2] communication.

By enabling European citizens to access, manage, and share their health data electronically (*primary use*), and facilitating its use for public interest, policy making, and research (*secondary use*), the EHDS seeks to harness the vast potential of European citizens' health data.

The primary goal of the EHDS is to empower patients to access their health data electronically and enable health professionals to consult patients' medical records, through secure and interoperable Electronic Health Records (EHRs), wherever they are in the EU. The already existing, although not yet widely used, cross-border digital EU infrastructure **MyHealth@EU**, will allow health professionals in different EU countries to safely access essential patient data, such as summaries, electronic prescriptions, medical imagery, and laboratory results. Having access to critical health information, including diagnoses and medication lists, would allow healthcare providers to quickly understand patient's medical history and provide quicker and more informed care. This would also reduce the need for unnecessary tests and enhance continuity of care.

Other than the use of health data for direct care, the EHDS also aims to harness the research potential of health data by making anonymised or pseudonymised data available for secondary use through a decentralised EU infrastructure called **HealthData@EU**. Data from health records, clinical trials, health claims, genetic information, and public health registries will be processed for public interest purposes,

[1] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Health Data Space, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0197

[2] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A European strategy for data, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066

including research, statistics, and policymaking, enabling advancements in treatments. Enhanced data sharing would also facilitate more effective research into care pathways, treatment efficacy, and the development of new medical innovations, such as predictive tools and AI applications, with the potential to ultimately improve patient outcomes and quality of life.

Figure 1: Legislative timeline of the EHDS Regulation

2. Analysis

2.1 PRIMARY USE OF HEALTH DATA

Chapter II of the EHDS regulation lays out comprehensive provisions regarding patients' rights related to the primary use of electronic health data, focusing on access, portability, and control. The framework strongly emphasises security and privacy, ensuring that all data sharing takes place within secure processing environments[3]. The EHDS is a decentralised system, operating as a network of interconnected systems, rather than a central repository. This architecture enables different systems across the EU to communicate securely and effectively, preventing the transfer of data through insecure channels like email. Instead, authorised users will access data through secure platforms specifically built to prevent unauthorised access or breaches. A key aspect of the EHDS is its emphasis on interoperability, facilitating the secure exchange of health data across different countries and

[3] A Secure Processing Environment is a protected system where sensitive data is processed in a way that prevents unauthorised access or tampering.

healthcare systems. The framework adheres to General Data Protection Regulation[4] principles, ensuring that all data processing aligns with strict European privacy standards. Below is an overview of the most relevant provisions related to primary use of health data in the EHDS regulation.

ACCESS TO ELECTRONIC HEALTH DATA

Many citizens and patients still face barriers when trying to access their electronic health records, both nationally and across borders. However, this is expected to change with the mandatory introduction of free electronic health records (EHRs) for all EU citizens. The EHDS will ensure that patients, or a representative of their choice, can access their health data electronically, at no cost, and immediately after it is recorded in an EHR system. This data will be presented in a consolidated, easily readable, and accessible format. The right to obtain a paper copy of the electronic health data will remain. It is also important to note that if personal health data has not been collected electronically prior to the application of the EHDS regulation, Member States may decide not to convert it into an electronic format.

The types of information included in EHRs will be:

- patient summaries
- electronic prescriptions
- electronic dispensations
- medical imaging studies and related reports
- medical test results, including laboratory and diagnostic reports, and
- discharge summaries.

Additionally, Member States will have the option to make more categories of personal electronic health data available for primary use, further expanding the scope of the EHDS.

DELAYED ACCESS TO ELECTRONIC HEALTH DATA

In cases where a healthcare professional determines that the patient's health may be significantly impacted by new medical findings, such as the diagnosis of a severe condition, Member States may implement measures allowing for delayed access to the patient's electronic health record. This temporary delay ensures that healthcare professionals have the opportunity to personally communicate and explain the findings to the patient. The primary objective is to provide professional guidance, preventing patients from encountering sensitive or potentially distressing information without adequate support or context.

DATA PORTABILITY

To facilitate the access and exchange of health data cross-border, EHDS will make sure that patients are able to access their health data wherever they are in the EU in an electronic format that can be recognised and accepted in all EU countries. Healthcare professionals in countries other than the patient's country of origin will have access to the data in their preferred language. To ensure this right

[4] 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), available at https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

to portability of health data, all Member States will be required to participate in cross-border digital infrastructure for the exchange of health data for healthcare delivery (**MyHealth@EU**).

Moreover, the EHDS regulation will allow patients to give access to or request a healthcare provider to transmit all or part of their electronic health data to another healthcare provider, social security or reimbursement services sector, free of charge.

RIGHT TO RECTIFICATION OF ERRORS AND INSERTING OF INFORMATION

The EHDS regulation enables patients to request changes of possible errors such as incorrect or incomplete information, immediately and free of charge, through an electronic health data access service. If necessary, health professionals responsible for the patient's treatment will be involved. This particular provision will be developed further at the national level.

Moreover, the EHDS will allow patients or their representatives to insert information in their own EHR, but without the possibility to directly alter the information inserted by health professionals. This information will be clearly distinguishable as inserted by the patient.

MONITOR AND RESTRICT ACCESS TO PERSONAL DATA

The EHDS will give patients the ability to limit healthcare providers' access to all or certain parts of their personal electronic health data. Patients who choose to exercise this right should also have the option to reverse their decision and will be informed that restricting access could affect the healthcare they receive. When access to electronic health data has been restricted by the patient, the health professionals will not be informed of the restricted content of those electronic health data. Patients will be able to allow access to certain parts of their personal health data while restricting access to other parts, as for example information on sensitive issues such as mental or sexual health.

Since the unavailability of restricted health data may impact the quality or provision of services, patients will have to accept responsibility for the fact that healthcare providers cannot consider the restricted data when delivering care. In critical situations, such restrictions could have life-threatening consequences and the access to personal health data will be allowed to protect vital interests during emergencies (*emergency override*).

Moreover, Member States may establish an absolute right for patients to opt-out from the access by anyone other than the person/institution who inserted the data, even without the emergency override. In this case, if a patient exercises this right to opt-out, healthcare providers will still document the treatment they provide in accordance with relevant regulations and retain access to the data they record. However, the data generated during the period of objection may not be accessible through the standard access services or MyHealth@EU. This application of this provision may vary across the EU Member States.

NOTIFICATIONS ON WHO HAS ACCESSED HEALTH DATA AND WHEN

Health data access services will offer detailed information on data access, including when and which entity or individual accessed specific information in patient's EHR. Individuals should also have the option to enable or disable automatic notifications about access to their health data through healthcare access services.

CREATION OF A DIGITAL HEALTH AUTHORITY

Each Member State must establish one or more digital health authorities responsible for the implementation and enforcement of Chapter II of the EHDS regulation at national level. The staff of DHAs must avoid any conflict of interest and must actively cooperate and consult with relevant stakeholders' representatives, including patients' representatives. The DHA will also be responsible for facilitating the exercise of the above-mentioned rights for persons with disabilities.
A person will have the right to lodge a complaint, individually or collectively with the DHA, which will then transmit the complaint to the relevant supervisory authority.

2.2 SECONDARY USE OF HEALTH DATA

Chapter IV of the EHDS outlines detailed provisions for the secondary use of electronic health data, establishing a secure and regulated framework for accessing data beyond direct patient care. Under this framework, public, private, and non-profit entities, as well as individual researchers, can access health data for various purposes, including research, innovation, policymaking, education, patient safety, regulatory activities, and personalised medicine. The goal is to contribute to the general interest of society by fostering advancements in healthcare through use and analysis of large health datasets.

The EHDS emphasises that the secondary use of data should benefit society by supporting the development of new medicines, medical devices, healthcare products, and services that are both affordable and accessible to EU citizens and improving their availability across all Member States. To facilitate this, the EHDS introduces **HealthData@EU**, a decentralised EU infrastructure that connects health data access bodies established in all Member States, enabling efficient and secure secondary use of health data. The framework includes clear guidelines to ensure that sensitive data is processed securely in anonymised[5] or pseudonymised[6] form, in compliance with GDPR standards. All data sharing occurs through secure platforms, preventing unauthorised access or breaches, and prohibiting the use of data for discriminatory decisions or marketing purposes. Chapter IV ultimately aims to create a balanced system that leverages health data for innovation and public health improvements while protecting individual privacy and promoting transparency. Below is an overview of the most relevant provisions related to secondary use of health data.

CREATION OF HEALTH DATA ACCESS BODIES (HDAB)

Member States will establish one or more Health Data Access Bodies, responsible for issuing permits for the secondary use of health data to data users who wish to process them for research, policymaking or public health monitoring (detailed list of these purposes is available below). Their role is to ensure that health data is only used for legal, ethical, and scientific purposes, with robust safeguards in place to protect patient privacy.

[5] A data protection technique where personal identifiers in a dataset are completely removed, ensuring to the maximum extent possible that natural persons cannot be re-identified by health data users.
[6] A data protection technique where personal identifiers in a dataset such as a person's name, social security number, or date of birth, are replaced with a unique code or identifier. This ensures that the individual cannot be easily identified without access to additional information (a "key") that links the code back to the person. While the data can still be used for analysis or research, the identity of the individual remains protected.

The staff of HDABs must avoid any conflict of interest and must actively cooperate and consult with relevant stakeholders' representatives, including patients' representatives. HDABs should publicly disclose information about the granted data permits, along with their justifications, the measures implemented to protect the rights of individuals, the methods available for individuals to exercise their rights concerning secondary use, and the outcomes resulting from the secondary use of the data. Additionally, they should publish biennial activity reports providing an overview of their activities, in order to promote transparency.

OBLIGATIONS FOR DATA HOLDERS

A health data holder in the context of the EHDS is an entity responsible for managing and providing access to electronic health data. This can include public and private healthcare providers, public authorities, research institutions, or companies offering or developing healthcare-related services, as well as any Union institution or body. Data holders are required to make electronic health data available upon request to health data access bodies within a reasonable timeframe, no later than three months from receiving the request. The EHDS regulation exempts natural persons, including individual researchers and legal persons that qualify as microenterprises[7], from the obligations on health data holders. However, the Member States will be able to override this exemption according to their national law. It is also important to note that health data holders may charge fees for making electronic health data available for secondary uses which should cover all or part of the costs related to the procedure for making the data available.

OBLIGATIONS FOR DATA USERS

Data users are individuals or entities, such as researchers, companies and authorities who access health data for secondary use upon the permit granted by a HDAB. Health data users can only process electronic health data for secondary use in accordance with the purposes contained in a data permit. Within 18 months of accessing and using the data, health data users are obliged to make public the results or output of secondary use, including information relevant for the provision of healthcare.

MINIMUM CATEGORIES OF ELECTRONIC DATA FOR SECONDARY USE

If requested, health data holders will have to make the following categories of electronic health data available for secondary use:

a) electronic health data from EHRs
b) data on factors impacting on health, including socio-economic, environmental and behavioural determinants of health
c) aggregated data on healthcare needs, resources allocated to healthcare, the provision of and access to healthcare, healthcare expenditure and financing
d) data on pathogens, impacting human health
e) healthcare-related administrative data, including dispensation, claims and reimbursement data
f) human genetic, epigenomic and genomic data
g) other human molecular data such as proteomic, transcriptomic, metabolomic, lipidomic and other -omic data

[7] According to the Commission Recommendation 2003/361/EC, a microenterprise is defined as an enterprise which employs fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million.

h) personal electronic health data automatically generated through medical devices
i) data from wellness applications
j) data on professional qualifications, experience, practice and status, specialisation and institution of health professionals involved in the treatment of a natural person
k) population-based health data registries (public health registries)
l) data from medical registries and mortality registries
m) data from clinical trials, clinical studies and clinical investigations
n) other health data from medical devices
o) data from registries for medicinal products and medical devices
p) data from research cohorts, questionnaires and surveys related to health, after the first publication of the related results, and
q) health data from biobanks and associated databases.

PURPOSES FOR WHICH DATA CAN BE PROCESSED FOR SECONDARY USE

Health data access bodies will only grant access for secondary use to a health data user where the processing of the data by that health data user is necessary for one of the following purposes:

a) public interest in the area of public and occupational health
b) policy- making and regulatory activities to support public sector bodies or Union institutions, bodies, offices or agencies and bodies, including regulatory authorities in the health or care sector
c) statistics, such as national, multi-national and Union level official statistics
d) education or teaching activities in health or care sectors at the level of vocational or higher education level
e) scientific research related to health or care sectors, that contributes to public health or health technology assessments, or ensures high levels of quality and safety of health care, of medicinal products or of medical devices, with the aim of benefitting the end-users, such as patients, health professionals and health administrators, including development and innovation activities for products or services, and training, testing and evaluating of algorithms, including in medical devices, in- vitro diagnostic medical devices, AI systems and digital health applications, and
f) improvements of the delivery of care, treatment of the optimisation of treatment and of the provision of healthcare, based on the electronic health data of other natural persons.

It is important to note that it will not be allowed to use the data to make decisions that negatively impact people, raise insurance costs, target health products at doctors or patients, or create harmful products or services.

OPT-OUT FROM DATA SHARING FOR SECONDARY USE

A right to opt-out from sharing health data for secondary use is introduced across all Member States. Patients must not be required to give any reasons for opting out and should have the possibility of reconsidering their choice at any time. However, Member States may establish mechanisms under national law to allow justified exceptions for the purposes such as scientific research conducted for significant public interest by public sector entities, including third parties acting on their behalf. These exceptions must respect the core of fundamental rights and be proportionate. The HDABs will assess the justifications for such exceptions.

CLINICALLY SIGNIFICANT FINDINGS

If researchers inform health data access bodies about findings that may impact the health of a patient whose data was used in the scientific research, the HDAB may inform the data holder who has to inform the patient or the relevant treating health professional about these findings. The patient can decide not to receive this information. The EHDS Board shall, in consultation and cooperation with relevant stakeholders, including representatives of patients, create guidelines to help health data users to determine what is intended to be clinically significant.

2.3 HEALTH RECORDS & WELLNESS APPLICATIONS

Chapter III of the regulation focuses on the interoperability and standards for EHR systems. The EHDS aims to standardise EHR systems to improve their interoperability, security, and privacy across the Union. The European Electronic Health Record Exchange Format[8] will serve as the basis for setting standards related to the registration and exchange of electronic health data, and the Commission will establish data quality requirements through implementing acts.

The regulation also introduces a self-certification scheme for EHR systems, supported by digital testing environments developed by the Commission. Manufacturers are required to use this environment for assessments before launching their products, and the results must be included in the technical documentation. EHR systems will be required to include an information sheet and clear, accessible instructions for use, particularly for individuals with disabilities.

Chapter III also introduces a mandatory labelling scheme for wellness applications claiming interoperability with EHR systems.

2.4 EHDS BOARD & STAKEHOLDER FORUM

The European Health Data Space Board, the main governance body, will be co-chaired by a Member State and the European Commission, and composed of representatives of the other Member States, Commission officials and observers. The Board aims to contribute to a consistent application of the rules throughout the EU, both for primary and secondary use. An EHDS stakeholder forum, which will advise the EHDS Board in the fulfilment of its tasks by providing stakeholder input on matters in the scope of the EHDS regulation, will be established. The forum will be composed of representatives of relevant health stakeholders, including patients, consumers, health professionals, industry, scientific researchers and academia.

2.5 DIGITAL HEALTH LITERACY

The EHDS regulation emphasises the need to improve digital health literacy for both patients and health professionals. Specifically for patients and the public, Member States are invited to prepare awareness-raising campaigns or programmes to inform patients and the public about the primary and the secondary use of the electronic health data as part of the EHDS framework. Special attention is recommended for vulnerable groups, including persons with disabilities, migrants, older and less

[8] To learn more about the European Electronic Health Record Exchange Format you can consult https://digital-strategy.ec.europa.eu/en/policies/electronic-health-records

digitalised people. Furthermore, the regulation advises providing patient-centric guidance to help patients use EHRs effectively, tailored to their specific digital literacy levels, and actions in ensuring that everyone has access to the necessary infrastructure.

IMPLEMENTATION TIMELINE

Significant disparities exist both between and within Member States regarding digitalisation progress and readiness. A major shared challenge is the lack of interoperability among electronic health data systems, which limits efficient data transfer, aggregation, and secondary use. To advance implementation, Member States must prioritise building robust national health data infrastructures, including harmonising technical standards, ensuring secure data sharing frameworks, and fostering collaboration between regional and national systems to bridge the digital divide. Below is a summary of which provisions will be implemented in the following years.

Within two years of the entry into force of the regulation (2027), the European Commission aims to adopt implementing acts and establish common specifications to ensure interoperability, data quality, and technical standards (templates for applications, requests & decisions; fees policies; data catalogues; data quality and utility label, etc) Member States will also designate HDABs and DHAs within this timeframe.

Within four years (2029), certain key types of electronic health information, like patient summaries and electronic prescriptions, will be made accessible for patients and healthcare providers under MyHealth@EU. Within 6 years (2031), these rules will expand to include more types of health data, such as medical imaging results like X-rays, lab test reports, and hospital discharge summaries.

Within eight years of entry into force (2033), the European Commission will conduct an evaluation of the implementation of the Regulation. If necessary, the report of the evaluation will include recommendations or proposals for necessary changes.

Within ten years (2035), all the rules about using health data for research and other secondary purposes will be fully in place. The EU will have a fully connected system, called HealthData@EU, to allow countries to share health data securely and effectively. This will mark the complete implementation of the regulation.

3. EPF recommendations for the implementation

In principle, EPF welcomes the final text of the EHDS regulation, recognising its potential to bring substantial benefits to patients, healthcare professionals, researchers and healthcare systems. However, as with any transformative policy, its implementation and its broader impact on health stakeholders will need to be continuously monitored and evaluated.

To ensure the successful realisation of the EHDS vision and mitigate any unintended consequences, EPF calls on the Member States and the European Commission to prioritise the following key actions during the implementation period:

1. **Accessibility and Usability**: EHR systems must be user-friendly, with clear interfaces that enable all patients, including those with disabilities, older people and those with limited digital

literacy, to manage their health data effectively. This includes intuitive navigation, language options, and accessibility features. Establishing channels for patients to report concerns, provide feedback, and shape ongoing improvements is crucial. In addition, to avoid digital burnout and negative impacts on patients and healthcare systems, EHR systems should be built in a way that reduces administrative burdens for healthcare professionals rather than increasing them.

2. **Transparency**: Patients should have transparent information in lay language on how their health data is collected, stored, used, and protected within the EHDS framework. Clear guidelines and communication protocols should be established to foster trust and accountability.

3. **Consent:** We welcome the provisions allowing patients to opt-out from the re-use of health data for secondary purposes and call for a harmonised implementation across Member States to ensure all patients enjoy the same rights. It is crucial to provide patients with complete and understandable information on the functioning of the mechanism as well as on potential drawbacks of exercising this right.

4. **Digital Health Literacy:** Promoting digital health literacy programs is essential, especially in underserved and rural communities. Resources and educational initiatives should be provided to empower individuals to navigate and benefit from electronic health services effectively. We call for a better involvement of and cooperation with initiatives like Data Saves Lives[9].

5. **Stakeholder Engagement**: The EHDS stakeholder forum should function as a true advisory board, whose feedback and recommendations are actively incorporated and acted upon, thereby avoiding a mere 'box-ticking' exercise. The same principle should be respected by HDABs and DHAs when collaborating with health stakeholders.

6. **Financial Considerations**: Addressing concerns about the financial burden on Member States and regions is crucial for sustainable implementation. Further clarifications are also needed on the digitalisation costs concerning healthcare professionals, both in terms of necessary equipment and training.

7. **Security and Privacy**: Ensuring state-of-the-art security measures to strengthen the protection and cybersecurity surrounding data storage and processing is of utmost importance.

8. **Minimising Legal Uncertainty:** It is critical to reduce legal uncertainties surrounding the implementation of EHDS, especially in cross-border health data sharing and usage, to ensure consistency, prevent misinterpretation, and streamline compliance.

[9] Data Saves Lives is a multi-stakeholder initiative with the aim of raising wider patient and public awareness about the importance of health data, improving understanding of how it is used and establishing a trusted environment for multi-stakeholder dialogue about responsible use and good practices across Europe. For more information and to discover DSL educational materials see here.

ABOUT EPF

The European Patients' Forum (EPF) is an umbrella organisation of patient organisations across Europe and across disease-areas. Our 78 members include disease-specific patient groups active at EU level and national coalitions of patients representing 21 countries and an estimated 150 million patients across Europe. www.eu-patient.eu

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.