Summary of the European Health Data Space Regulation

Abdellahi El Moustapha

1 Introduction

The **European Health Data Space (EHDS)** is a major EU initiative to empower individuals with control over their health data and to enable the safe exchange and use of health data for societal benefit. Established by Regulation (EU) 2024/... on the European Health Data Space, it is a cornerstone of the European Health Union, building upon the foundations of data protection (GDPR) and the EU's digital strategy. The EHDS creates a common framework of rules, standards, and infrastructure for health data across the EU, with twin objectives: improving **primary use** of electronic health data – i.e. patient access to and exchange of their own health records for healthcare delivery – and enabling **secondary use** of electronic health data – i.e. reuse of health data for research, innovation, policy-making, public health, and other purposes that benefit society.

This summary outlines the key provisions of the EHDS Regulation, including individuals' rights, obligations of various actors, mechanisms for data sharing, and governance structures for both primary and secondary uses of health data.

2 Primary Use of Data

Primary use refers to the use of personal health data in the context of healthcare delivery. The EHDS strengthens individuals' control and improves the flow of health information for patient care across Member States:

- **Individual Access:** Individuals have the right to immediate, free *electronic access* to their personal health data through digital health portals. Access covers a set of *priority health data categories* (patient summaries, e-prescriptions/dispensations, medical images and reports, lab results, and discharge reports) in a user-friendly format. Patients can download copies of their data and share them with healthcare providers of their choice. Exceptions allowing short delays are permitted only in cases where instant access would likely cause serious harm (e.g. delivering a severe diagnosis without clinical support).
- **Restricting Access:** Individuals can restrict health providers' access to parts of their electronic health data, though they are warned this may impact care quality. Any such restriction is invisible to providers (who simply see the data as unavailable). Member States must establish safeguards for these cases (and may allow "break-glass" access by clinicians in life-threatening emergencies despite a restriction).
- **Data Portability for Care:** The EHDS extends data portability: patients can have their health data transmitted directly between healthcare providers, including across borders, in a common interoperable format. For example, at a patient's request, a hospital can send medical records or an e-prescription from one Member State to another through the European infrastructure. Providers receiving such data must accept it and be able to read it.
- **Audit Trails:** Patients have the right to know who has accessed their electronic health data. They can receive logs or notifications showing which healthcare professionals accessed which data and when, enhancing transparency and trust.

Healthcare providers are obligated to support these rights. They must use certified EHR systems that can export data in the European Electronic Health Record Exchange Format and connect to national health information networks. Providers are required to record health data electronically (at least the priority categories) and update records in a timely way. No fees may be charged for sharing or accessing patient data for healthcare purposes under the EHDS.

To enable seamless **cross-border exchange** for primary use, the regulation establishes **MyHealth@EU**, a Europe-wide digital infrastructure for health data exchange. Each Member State designates a National Contact Point for Digital Health, which connects to MyHealth@EU. Through this network, health data like patient summaries and e-prescriptions can flow securely between countries. For example, a doctor in Member State B can retrieve a visiting patient's records from Member State A via MyHealth@EU, and a pharmacy can dispense a prescription issued in another Member State. Figure 1 illustrates the primary use data-sharing setup.

Figure 1: Primary use of health data: patients and providers access and share electronic health records across borders via MyHealth@EU. Patients use national electronic health data access services (portals) to view/download their data (dashed arrows), while healthcare providers retrieve necessary records from other Member States through National Contact Points connected to MyHealth@EU (solid arrows).

Member States must set up **digital health authorities** to implement these primary use provisions. These authorities oversee the national deployment of patient access services and provider access systems, ensure interoperability (adopting the European EHR exchange format standards), and coordinate with other countries through MyHealth@EU. They also promote digital health literacy and training for healthcare professionals, ensuring that both patients and providers can effectively exercise the new rights and tools.

3 Secondary Use of Data

Secondary use involves the processing of electronic health data for purposes other than direct care. The EHDS establishes a legal framework to allow such reuse under strict conditions, ensuring privacy and security:

- **Permitted Purposes:** Access to health data for secondary use is allowed only for defined objectives in the public interest. These include public health surveillance and crisis response, government health policy and planning, official statistics, education and training in health/care, and scientific research and innovation in health (e.g. epidemiological studies, clinical trials, development of medical AI). Using data for purposes adverse to individuals (such as insurance underwriting, employment decisions or marketing) is prohibited. All secondary processing must serve public interest goals or general knowledge advancement in health. *Furthermore, a wide spectrum of health datasets is made available for these secondary purposes – from EHR clinical records and claims data to health registries, biobank datasets, and genomic information – ensuring that data users can draw from comprehensive sources under uniform safeguards.*

- **Data Minimisation and Privacy:** Personal health data for secondary use must be handled in a privacy-preserving way. Data are typically *pseudonymised* (stripped of direct identifiers) before use. The regulation bans any attempt to re-identify individuals. Data analysis is generally done within secure controlled environments, and only aggregated or anonymised results can be taken out, preventing misuse of raw data.

- **Consent and Opt-Out:** While the EHDS creates a lawful basis for secondary use without individual consent (for important public interest projects), it gives individuals a right to **opt out** of having their data included. Each Member State must offer citizens a simple way to object to secondary use of

their health data. If a person opts out, their data cannot be made available for secondary purposes (with limited exceptions—national law may allow certain critical public-interest research by public institutions to still include all data, under strict safeguards). Individuals are not required to give a reason for opting out.

To operationalize secondary use, the EHDS requires each Member State to designate a **Health Data Access Body** (HDAB). This body is the gatekeeper and facilitator for secondary data requests:

- **Data Permit System:** A researcher or other authorized party (the *data user*) who wants to analyze health data must apply to the HDAB, specifying the purpose and data needed. The HDAB evaluates the request: it verifies that the purpose is allowed, checks that only the necessary data are requested, and ensures compliance with technical and ethical standards. If approved, the HDAB issues a **data permit** that details what data can be used and for what purpose.
- **Secure Access Environment:** Rather than transferring raw datasets to data users, the HDAB provides a controlled *secure processing environment* where the approved data can be accessed and analyzed. Data from various *data holders* (hospitals, databases, registries, etc.) are brought into this environment for the permitted analysis. The data user can perform computations but cannot remove any personal data from the platform. Only results (aggregate statistics, research findings) that pass disclosure controls leave the environment.
- **Oversight and Responsibilities:** Data holders are obliged to make requested data available to the HDAB when presented with a valid permit. They must cooperate by preparing and transmitting the needed pseudonymised datasets. Data users must use the data only for the permitted purpose and adhere to privacy and IT security rules. The HDAB monitors compliance and can audit usage. Any breach (like attempted re-identification or unauthorized use of data) can lead to sanctions, including revoking permits or excluding the offender from future access.

Importantly, the EHDS facilitates **cross-border secondary use** through a federated infrastructure called **HealthData@EU**. Health Data Access Bodies in different Member States will coordinate and share data for multinational projects. For instance, a researcher in Country A can request data from multiple countries; the HDABs in those countries will jointly review the request and provide access via connected secure environments. HealthData@EU acts as a network connecting national HDAB platforms, promoting Europe-wide research while keeping data protected. International access by entities in third countries is permitted only under equivalent standards and where allowed by EU/global agreements (ensuring no lower data protection standards apply).

Figure 2 illustrates the secondary use process.

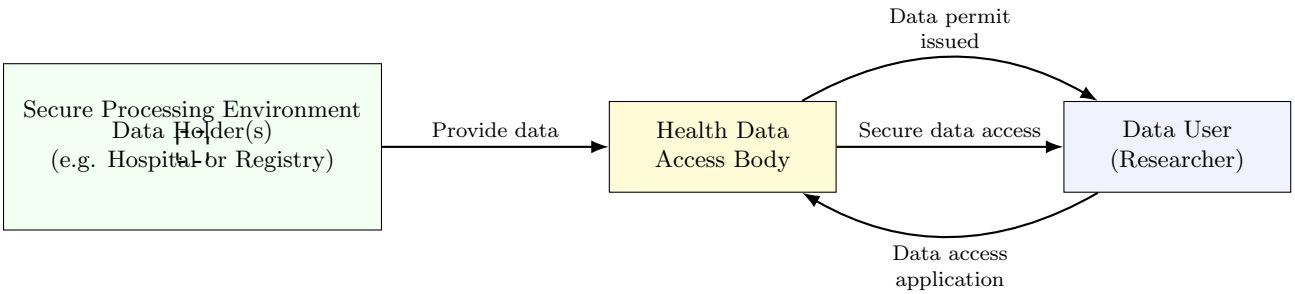

Figure 2: Secondary use of health data: Data users (such as researchers) apply to the Health Data Access Body (HDAB) for permission to use health datasets for an allowed purpose. If approved, the HDAB gathers the necessary data from relevant data holders and makes them available in a secure environment. The data user analyzes the data within this environment; only non-identifying results leave the platform.

4 Governance and Infrastructure

The EHDS creates a multi-layered governance structure:

- **National Level:** Member States establish both a *Digital Health Authority* (for primary use and EHR systems) and a *Health Data Access Body* (for secondary use). The digital health authority is responsible for implementing individuals' data rights, setting up national electronic health data access services (patient portals), ensuring healthcare providers and EHR systems comply with interoperability and security requirements, and serving as the National Contact Point connecting to MyHealth@EU. The Health Data Access Body handles secondary use requests as described and enforces conditions on data users and data holders. These bodies coordinate with data protection authorities to ensure alignment with privacy laws.

- **Cross-Border Infrastructure:** At the EU level, the Commission provides and oversees **MyHealth@EU** (for primary data exchange) and **HealthData@EU** (for secondary data federation). MyHealth@EU comprises the central platform and Member States' national contact points, enabling real-time exchange of patient data between countries. HealthData@EU interlinks national HDAB systems, allowing queries and studies to span multiple countries' datasets. The Commission sets technical standards and cybersecurity requirements, and performs compliance checks for connecting nodes.

- **European Coordination:** A **European Health Data Space Board** (EHDS Board) will be established, with representatives from all Member States and the Commission. This Board will facilitate consistent implementation by issuing guidelines, sharing best practices, and resolving cross-border issues. It can form subgroups focusing on primary use (infrastructure, interoperability) and secondary use (data access procedures, data quality standards). A stakeholder forum (including patient groups, researchers, industry) will advise the Board. The EHDS Board's work is without prejudice to the powers of independent data protection authorities, but it will collaborate with them as needed.

- **Supportive Measures:** The EHDS mandates capacity-building initiatives. The Commission will support training programs for health professionals to use the new digital tools and will assist Member States in raising public awareness about the EHDS. Member States are encouraged to run campaigns informing citizens of their new data rights and the benefits of data sharing. EU funding and public procurement will also be leveraged: public sector projects should use EHDS-compliant systems, and adherence to EHDS standards can be required when spending EU funds on health IT.

5 EHR Systems and Interoperability

To ensure that health data can flow smoothly and securely, the regulation introduces EU-wide requirements for **Electronic Health Record (EHR) systems** and certain health applications:

- **Essential Requirements:** EHR systems (software used by healthcare providers to manage patient data) must meet interoperability and security requirements defined by the EHDS (see Annex II of the Regulation). In particular, every EHR system must implement two harmonised EU components: a **European Interoperability Module** (to support the European EHR exchange format and connectivity with MyHealth@EU) and a **European Logging Module** (to record user access events for auditability). General-purpose IT tools (like word processors) are exempt, but any product marketed as an EHR system in the EU must include these components.

- **Standards and Specifications:** The European EHR exchange format is standardized via implementing acts – specifying common datasets (fields and structure for health records), code systems (e.g. ICD, SNOMED CT for diagnoses; LOINC for lab results), and technical protocols for exchange. All EHR systems must be able to export and import the priority data categories in this format. The Commission can update these specifications as needed to keep up with technological and international developments.

- **Conformity Assessment:** EHR systems are subject to an EU conformity assessment similar to other regulated products. However, instead of third-party certification, the EHDS uses a *self-certification* approach. Manufacturers must test their EHR system's harmonised components in a **European digital testing environment** before placing the product on the market. The testing environment (developed by the Commission and implemented by Member States) provides automated checks that the interoperability and logging functions work correctly. Test results are included in the system's technical documentation. If the EHR system conforms to all requirements, the manufacturer issues an EU Declaration of Conformity and affixes the CE marking to the product, indicating compliance. Member States cannot impose additional interoperability requirements that would block CE-marked EHR systems from their market (although they may set national rules on aspects not covered by the EHDS, such as additional functionalities).

- **Market Surveillance and Safety:** National authorities (often the digital health authorities) will act as market surveillance authorities for EHR systems. They can audit products, review technical documentation, and investigate complaints. If an EHR system is found non-compliant or poses significant risks (for example, a logging failure or cybersecurity flaw), authorities can require corrections, suspend the product from the market, or recall it. Manufacturers, importers, and distributors of EHR systems are obliged to cooperate with authorities, remedy any non-conformities, and report serious incidents (such as a security breach involving the EHR) to the authorities.

- **Wellness Applications:** The regulation also addresses *wellness apps* (health-related software for personal well-being, not classified as medical devices). Such apps are not mandated to undergo certification, but if they claim to be interoperable with EHR systems, they must transparently show it. A voluntary **labeling scheme** is introduced: a wellness application that meets the EHDS interoperability requirements (e.g. uses the standard format and coding for data) can display a label indicating compliance. This allows consumers and providers to identify apps that will integrate well with official EHR systems. Member States can encourage use of this label to promote trustworthy health apps, but cannot require stricter national certification for interoperability than the EHDS standards.

Overall, these measures aim to create a single market for digital health products. An EHR system certified in one country will be recognized across the EU, fostering competition and innovation while ensuring baseline functionality (like data portability, security, and audit logging) everywhere.

6 Rights and Obligations Summary

The EHDS Regulation grants new rights to individuals and imposes responsibilities on data handlers. Table 1 summarizes key rights of natural persons and corresponding obligations:

Beyond the above, various actors have direct obligations under the EHDS:

- **Healthcare providers** must use EHDS-compliant EHR systems, connect to national and EU digital health networks, and not refuse health data from other Member States. They are required to enter and update patient data electronically and facilitate patients' exercise of their rights (e.g. by enabling portal access and data transfer).

- **EHR system manufacturers** must ensure their products meet the EHDS requirements, undergo the prescribed testing, and carry the CE mark. They must monitor their products in use and address any issues (with potential liability if their product fails to comply).

- **Health data holders** (such as hospitals, labs, health registries) must make datasets available for secondary use when a valid data permit is presented. They cannot unjustifiably refuse an HDAB request (claims of intellectual property or trade secrets are mediated by the HDAB to balance proprietary rights with the public interest). Data holders also must assist in ensuring data quality (providing metadata about the datasets).

- **Health data users** (researchers, public health authorities, etc.) must use the data only for the approved purpose and follow all conditions in the data permit. They must keep data secure and

Rights of Individuals	Obligations on Entities
Immediate electronic access to health data (free, across borders)	Healthcare providers must provide priority data to patients quickly via electronic health portals, with no charges.
Data portability (transfer to chosen provider)	Providers must transmit and accept electronic records (in the EU exchange format) from other providers or countries without fees or undue delay.
Secondary use of data (with opt-out)	Health Data Access Bodies and data holders must make health data available for permitted research and public interest uses; data users must protect privacy (no re-identification) and honor any individual opt-outs.
Privacy controls and transparency	Patients can restrict provider access to parts of their data; providers must respect restrictions except for emergency need. All accesses to records are logged and patients can see who viewed their data.
Correction of errors	Individuals can request correction of inaccurate data. Data controllers (e.g. hospitals) must rectify errors. Patient-supplied additions to records are kept identifiable (marked as patient-provided).

Table 1: Key EHDS rights for individuals and corresponding obligations on healthcare providers, data holders, and data users.

confidential, and they may need to share their research results or insights (in anonymized form) with the HDAB or the public as appropriate. Any attempt to misuse data can lead to loss of access and legal penalties.

Enforcement of these rights and obligations is carried out through a combination of national and EU mechanisms. Data protection authorities will continue to enforce GDPR obligations (with the EHDS complementing those rights), while digital health authorities and health data access bodies enforce the specific EHDS provisions. Penalties for non-compliance can include fines and corrective orders. The EHDS Board will help ensure harmonized enforcement across the EU.

Conclusion

The European Health Data Space Regulation heralds a new era for digital health in Europe. By empowering patients with access and control, mandating interoperability of systems, and creating a safe pathway for researchers to use data, the EHDS seeks to deliver tangible benefits: better clinical care through informed data sharing, accelerated medical research and innovation, and more effective health policies based on evidence. As Member States implement this regulation, the EHDS will foster a **trustworthy, unified health data environment** that balances innovation with privacy, ultimately contributing to high-quality, resilient healthcare systems across the EU.