European Health Data Space Regulation (EHDS)

This past March 5th, Regulation (EU) 2025/327 (hereinafter, the "Regulation") was published in the OJEU, which establishes the regulatory framework of the European Health Data Space (hereinafter, the "EHDS"), with the aim of ensuring secure and efficient access to electronic health data in the European Union.

Entry into force

The Regulation will enter into force as from March 26th of this year. However, its applicability will be progressive: the general provisions will be applicable as of March 26, 2027, while some specific obligations will not become applicable until March 2029 and March 2031.

Objectives of the Regulation

The main objective of the Regulation is to create a common framework to enable secure, interoperable and efficient access to electronic health data across the EU, both to improve healthcare (primary use) and to foster research, innovation and data-driven policy-making (secondary use).

Among its specific goals, the EHDS seeks to strengthen the control of patients' health data, facilitating the interoperability of electronic health record (hereinafter, "EHR") systems, and establishing quality and security standards for data processing. It also promotes the reuse of health data for scientific and social purposes, respecting fundamental rights and the protection of personal data, in line with the GDPR.

Scope of application

▶ Individuals who generate electronic health data

will have specific rights over their electronic health data as will be covered later in this document.

▶ Health data holders

Article 2(2)(t) of the Regulation defines health data holders as any natural or legal person, public authority, agency or body that meets the following criteria:

- **Affected Sectors:** Operate in the health or care sectors, including reimbursement services, or develop products or services intended for these sectors.
- **Data Control:** Are responsible for the processing of personal health data (as controllers or co-controllers) or have the technical capacity to make non-personal health-related data available.
- **Examples of data subjects:** Healthcare providers (hospitals, clinics, physicians), manufacturers of wellness apps (wellness apps) that process health data or health-related research institutions.

About BDO Abogados

We are an international law firm committed to delivering superior quality and value services to drive the success of our clients around the world.

We adapt our work approach, fees and equipment according to the specific needs that each case requires, having a large capacity of resources to address any legal challenge effectively and efficiently. Your success is our priority.

People helping people achieve their dreams.

Contact

Marina Fontcuberta

Director | Digital Law
marina.fontcuberta@bdo.es

www.bdo.es

Article 2(2)(t): "«health data holder » means any natural or legal person, public authority, agency or other body in the healthcare or the care sectors, including reimbursement services where necessary, as well as any natural or legal person developing products or services intended for the health, healthcare or care sectors, etc."

▶ Entities in the health and care sector

Including hospitals, pharmacies and other healthcare providers, are required to record, process and share electronic health data in interoperable formats, such as the European Electronic Health Record Exchange Format (hereinafter "EEHRxF") (Articles 13, 14 and 15). They must also ensure data security and quality, as well as comply with requests for access and secondary use of data by health data access agencies (Articles 57 and 60).

▶ Developers and suppliers of EHR systems

Must comply with the essential interoperability[1] and safety requirements set out in the Regulation (Articles 25 and 36). This includes implementing harmonized software components for interoperability and registration, obtaining the CE conformity mark and registering the systems in the EU database (Articles 37, 39 and 49). In addition, they must subject their products to automated testing in digital test environments before they are placed on the market (Article 40).

Regulation of AI Systems

The Regulation addresses the interaction between electronic health record systems and AI systems, establishing specific requirements to ensure interoperability, security and protection of electronic health data.

▶ Interaction with the Artificial Intelligence Regulation (AI Act)

LEHR systems that incorporate AI functionalities, such as emergency triage tools, will be subject to both EHDS and AI Act requirements. This includes the classification of such systems as "high-risk systems" under the AI Act, which implies the need to comply with strict security, transparency and risk assessment requirements (Article 27.2 of the EHDS and Article 6 of the AI Act).

▶ Compliance and Registration

Manufacturers of EHR systems that integrate IA must demonstrate compliance with the essential requirements of both regulations. To simplify procedures, the EHDS allows for coordinated registration in the AI Act high risk systems databases and the EHDS EHR systems database (Article 49.3 of the EHDS).

▶ Conformity Assessment

The regulation states that conformity assessment procedures should be organized in a way that minimizes the administrative burden for EHR system manufacturers. This includes the possibility of joint or coordinated assessments to meet the interoperability and safety requirements of both regulations (Article 36 of the EHDS and Article 71 of the IA Act).

▶ Data Protection and Security

EHR systems with IA must ensure the protection of personal electronic health data, complying with the provisions of the GDPR and the specific security measures of the EHDS, such as the use of secure processing environments (Article 73 of the EHDS).

Correlation with the GDPR

Rights over electronic health data

The EHDS complements and extends the rights established in the GDPR, adapting them specifically to the field of electronic health data, with the aim of ensuring greater protection and control by patients.

▶ Reinforcement of existing rights

- **Rectification right:** The EHDS reinforces the right of rectification (Article 6 EHDS), already recognized in the GDPR (Article16), by establishing specific mechanisms for patients to request correction of incorrect information in their electronic health data.

[1]Systems must be capable of importing and exporting data in the European Electronic Health Record Exchange Format (EEHRxF).

- **Portability right:** The EHDS (Article 7 EHDS) extends the one provided for in the GDPR (Article 20), by requiring that health data can be transferred in an interoperable format, such as the EEHRxF format. This facilitates the exchange of data between health systems and ensures its effective use.

▶ New security and transparency guarantees

- **Right to limit access: t**he EHDS introduces the right of patients to restrict access to specific parts of their health data (Article 8 EHDS), reinforcing confidentiality and protection against unauthorized access, in line with the security principle of the GDPR (Article 5.1.f).
- **Right to obtain information on access:** the EHDS establishes that patients have the right to know who has accessed their health data and when (Article 9 EHDS), extending the right of access of the GDPR (Article 15). It also strengthens patients' rights by guaranteeing them immediate and free access to priority categories of data[2] through electronic health data access services.

▶ Introduction of new rights

- **Right to add information:** one of the main innovations of the EHDS is the right of patients to add information to their electronic health record (Article 5 EHDS). This right, not contemplated in the GDPR, allows patients to supplement their medical records with relevant data, such as information from wellness apps, encouraging their active participation in the management of their health[3]

Responsibility and safety measures

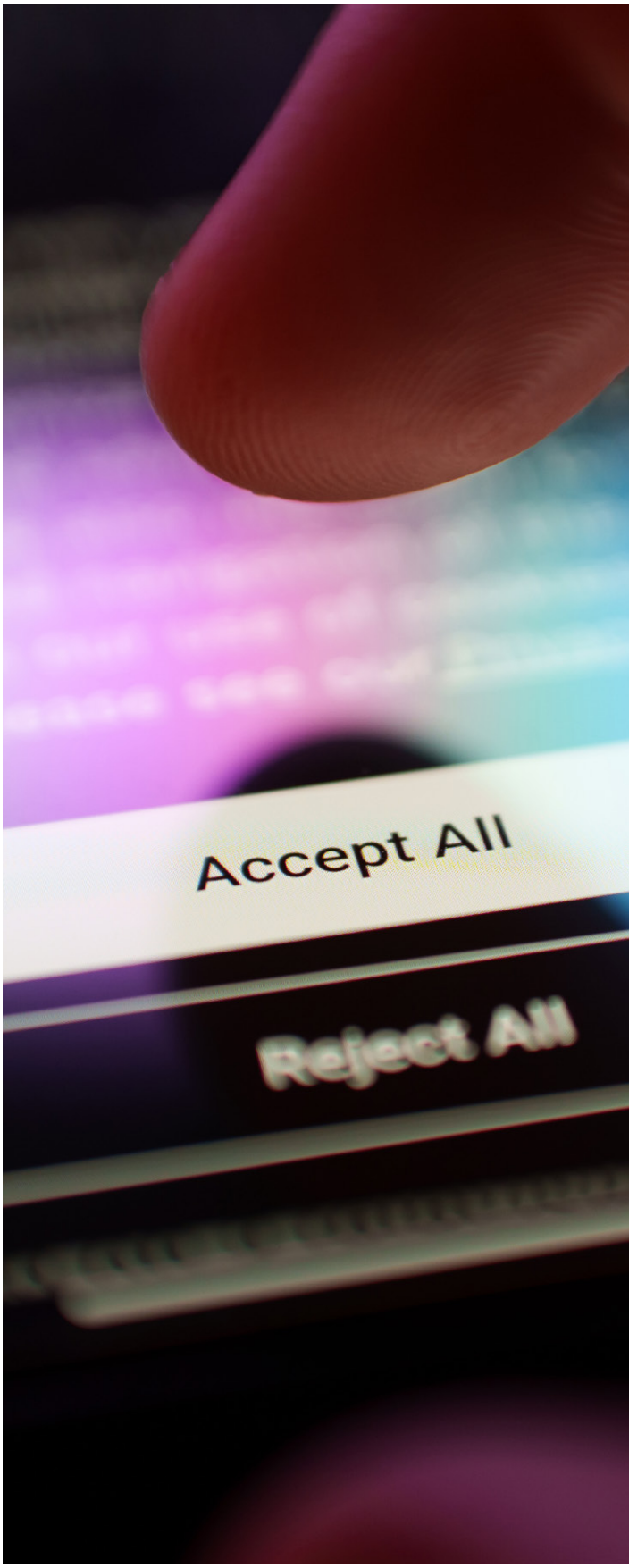
Both the GDPR and the EHDS stress the importance of the responsibility of data controllers (Article 24 GDPR) and the need to adopt security measures to protect data against unauthorized access, alteration or loss.

Compensation for damages

The GDPR (Article 82) guarantees the right to receive full compensation for damages, including moral damages, from the controller or processor in the event of a breach of data protection rules. The EHDS reinforces this principle by establishing clear mechanisms to protect patients' rights in the area of electronic health data.

EHDS implementing acts

Implementing acts are based on Article 291 of the TFEU, which allows the European Commission to adopt measures to ensure the uniform application of EU legal acts. In the case of the EHDS, implementing acts are essential to develop technical specifications, interoperability requirements and security measures.



[2]Pursuant to Article 14 of the EHDS, the priority categories of personal electronic health data will be the following: patient summaries; electronic prescriptions; electronic dispensations; medical imaging studies and related imaging reports; medical test results, including laboratory and other diagnostic results and related reports; and discharge reports.

[3]The introduction of information by individuals or their representatives does not imply that they can directly modify the electronic health data entered by health professionals.

Article 105 of the Regulation establishes a timetable for the adoption of implementing acts, which must be adopted within two years from March 26, 2027. The most relevant implementing acts include:

- Technical specifications for EEHRxF (Article 15).
- Data quality requirements for primary use (Article 13).
- Common specifications for harmonized components of EHR systems (Article 36).
- Requirements for secure treatment environments (Article 73).
- Requirements for the MyHealth@EU cross-border infrastructure (Article 23).
- Templates for data access requests and data permissions (Article 70).
- Data quality and utility label (Article 78).

Conclusions

The EHDS represents a significant advance in the regulation of electronic health data processing in the European Union. It strengthens patients' rights, establishes clear requirements for electronic health record systems and promotes the secondary use of data for research and innovation, especially in the field of artificial intelligence.

The various stakeholders involved, from patients to AI system manufacturers, will need to adapt to these new requirements to ensure regulatory compliance and take advantage of the opportunities it offers.

Keep this in mind:

- **Wellness applications.**
- **Role definition: data controller, data co-controller and data processor.**
- **Introduction of new rights.**