EU Health Data Space Act (EHDS)

TaylorWessing

Purpose

The EHDS Regulation aims to create a comprehensive framework for accessing and utilising electronic health data, fostering interoperability and robust governance. It seeks to enhance the primary and secondary use of health data, thereby improving healthcare services, advancing research and innovation, and supporting informed policymaking across the European Union.

Scope

The EHDS complements existing data protection laws, establishes common standards for electronic health records and wellness applications, and provides mechanisms for the cross-border exchange and secondary use of health data. It ensures coordinated governance at national and EU levels, facilitating secure, efficient, and legally compliant health data processing.

Application

The EHDS is expected to be finalised by the end of 2024. It will come into effect 2 years later. Specific provisions will apply 4 years later for certain categories of personal electronic health data and European Health Records (EHRs) for other categories. Implementing legislation must be adopted within 2 years. Chapter IV on secondary use will apply 4 years after entry into force.

Primary use of electronic health data by patients	The EHDS grants natural persons several rights regarding their personal electronic health data: immediate, free access to their data in a readable format and the ability to download an electronic copy; establishment of services for data access and proxy authorisations by Member States; the right to add information to their EHR, clearly distinguishable from professional entries; online requests for data rectification; the ability to transfer data to other healthcare providers, including cross-border transfers; the right to restrict access to their data with appropriate safeguards; notifications of who accessed their data, including details like date and time; and the option to opt-out of data sharing, with reversible mechanisms and specific safeguards provided by Member States.
Primary use of electronic health data by health professionals	**Health professionals**, defined as doctors, nurses, dental practitioners, midwives, pharmacists, or other regulated healthcare professionals, will have access to relevant personal electronic health data of patients under their treatment, including cross-border access facilitated through specified infrastructure. This access includes priority data categories and must adhere to national rules, considering restrictions imposed by individuals. Health professionals' access is logged, and any vital interest access must be documented and safeguarded. Member States must ensure that health professionals can access electronic health data, including for cross-border care, using recognised electronic identification means, with data presented in a user-friendly manner. Individuals have the right to use electronic identification for health data access, and the Commission will establish requirements for cross-border identification and authentication mechanisms. These mechanisms will support data transferability across borders. Member States and the Commission are responsible for implementing these mechanisms. Lastly, healthcare providers cannot charge for making personal electronic health data available, so there are no fees for data sharing or access for data subjects.
Prerequisites and obligations for EHR systems and wellness applications	The EHDS sets prerequisites and obligations for EHR systems and wellness applications to ensure safety, interoperability, and compliance. EHR systems must include a European interoperability component and a European logging component, and these systems can only be marketed or used if they comply with these components and the EHDS provisions. Wellness applications, defined as any appliance or software for processing electronic health data to provide individual health information or care for non-healthcare purposes, can claim interoperability with EHR systems. ■ **Manufacturers** must ensure their EHR systems meet essential requirements and common specifications, prepare and maintain technical documentation and an EU declaration of conformity, provide an information sheet and clear usage instructions, affix the CE marking, and register EHR systems and wellness applications in the EU database before marketing them. They must take corrective actions for non-compliant systems, cooperate with market surveillance authorities, and establish channels for complaints, maintaining a register of complaints and recalls. ■ **Importers** are responsible for ensuring EHR systems comply with essential requirements before market placement, verifying that manufacturers have the necessary documentation and CE marking, providing their contact information, and ensuring systems are accompanied by clear instructions. They must also keep documentation available for market surveillance authorities, cooperate with them, and maintain accessible channels for complaints. ■ **Distributors** must verify that EHR systems have the required conformity documentation and CE marking before market availability, ensure systems are accompanied by clear instructions, communicate necessary corrections to manufacturers or importers, cooperate with market surveillance authorities, and maintain records of complaints. ■ **Authorised representatives**, appointed by manufacturers outside the Union, must keep the EU declaration of conformity and technical documentation available for market surveillance authorities, inform manufacturers of non-conformity issues or complaints, and cooperate with market surveillance authorities, ensuring detailed arrangements in case of representation change.
Secondary use of data	The EHDS outlines conditions for the secondary use of electronic health data, specifying lawful purposes, prohibited uses, and data entailed. Secondary use means the processing of health data for purposes beyond individual patient care, such as research, policy making, and public health. Lawful purposes include public and occupational health activities, policy making, regulatory activities, official statistics, education, scientific research, and improving healthcare delivery. Only public sector bodies and EU institutions can access data for public health surveillance, quality and safety assurance of healthcare, and statistics. Prohibited uses of secondary data include making decisions detrimental to individuals or groups based on health data, influencing job offers or terms of goods and services provision, including insurance or credit conditions, advertising or marketing, and developing harmful products or services, such as illicit drugs or addictive products. Activities conflicting with ethical provisions under national law are also forbidden. Data for secondary use includes electronic health records, socio-economic and behavioural health determinants, aggregated healthcare data, pathogen data, genetic and molecular data, data from medical devices and wellness applications, professional health data, registry data, clinical trial data, and biobank data. Health data holders must inform access bodies of data protected by intellectual property rights or trade secrets. Compensation for making data available is not required.
Duties of health data holders	A health data holder is any natural or legal person, public authority, agency, or body in the healthcare or care sectors, including reimbursement services, wellness application developers, research entities, or mortality registries, with the right or obligation to process personal electronic health data for various purposes, or control non-personal electronic health data through technical design. Health data holders must make relevant electronic health data available to health data access bodies upon request within three months and update dataset descriptions annually. They must ensure data quality and utility labels are accurate and provide access to non-personal electronic health data through trusted open databases. Exemptions apply to individual researchers, natural persons, and micro-enterprises, though Member States may extend obligations to these entities. Health data holders are considered controllers for disclosing personal electronic health data to access bodies, who then become controllers for processing the data. The access body acts as a processor for users when providing data through secure environments.
Duties of health data users	A health data user is a natural or legal person, including EU institutions, granted lawful access to electronic health data for secondary use under a data permit, data request, or access approval. Health data users may only access and process electronic health data for secondary use with a data permit or request. They are prohibited from re-identifying individuals, must ensure data remains within secure environments, and cannot share it with unauthorised third parties. Users must publish the results of data use within 18 months, containing only anonymous data, and inform access bodies of significant health findings. They must acknowledge data sources and the EHDS context, cooperate with health data access bodies, and support the publication of results on access bodies' websites. Users are deemed controllers for processing pseudonymised personal electronic health data within secure environments under their data permits, while access bodies act as processors for users' data processing in secure environments.