



What's next for data protection in healthcare in the EU?

Safeguarding health data while facilitating its use for creating and driving more resilient and sustainable healthcare systems in the context of the European Health Data Space

Authors: Petra Wilson and Anett Molnar
For the empirica team

October 2024

Images: freepik.com - rawpixel.com, marta1995k

Health data holds significant value in its direct use when individuals receive healthcare services, and in its secondary use for population level health management, care services planning and life sciences research. In the context of care provision, making the right data easily accessible at the right time will drive safer and more efficient healthcare; while the re-use of data created through care provision for research, innovation, healthcare planning and policy-making has huge beneficial potential.

*The proposed **European Health Data Space Regulation**¹ seeks to make health data more accessible for both primary use in care provision and secondary use for research and innovation. In achieving this aim three often competing objectives need to be met. A well-functioning European Health Data Space will need to ensure that the EU **internal market in digital health services** can thrive, both for patients who wish to use them and care providers as well as industry who wish to supply them. However, the use of the digital health services must respect the **right of Member States to organise their own healthcare systems**, thus demand good alignment of EU and national laws. Also, as the use of European Health Data Space necessarily involves the use and re-use of data relating to patients and citizens, the **rights and interest of patients in accessing and controlling health data** concerning them must be observed and their exercise facilitated.*

The complex relationship both in law and in practice in meeting these three objectives demands that efforts are made to build a thorough understanding of how these competing rights may be balanced in order that confidence and trust in the use and re-use of health data grows across the society as a whole.

The EU legal landscape for digital health solutions

The EU legal landscape within which digital health solutions exist may be seen as straddling three broad areas of EU legislation - public health, internal market, data protection - which will at times be in competition with one another.

In terms of healthcare provision, the EU does not have a direct legal competence (the right to enact legislation) in the area of healthcare provision. Its role is limited to complementing the Member State actions in providing healthcare within their jurisdictions; each Member State has the right to organise the operation of its own healthcare system. However, providing healthcare in a Member State requires healthcare professionals, medicines, medical devices and all manner of healthcare related services. These people, products, services and investments function within the EU internal market and are governed by the principles of the freedom of movement

of workers, services, goods and capital. Rights which in turn create the freedom of patient to use healthcare services across the borders, as well as industry to bring products such as medical devices to market across the EU on a level playing field. When the healthcare services provided through the use of internal market freedoms use or include digital health services, a third element comes into play, that of data protection. For each time a patient interaction with the healthcare system generates data, the rights of the patient in having access to, control of and a right to the protection of their privacy arises.

Digital health therefore creates not only huge potential for building accessible, efficient and sustainable healthcare systems, but also new challenges for balancing the right of the Member State to organise its own healthcare system, the objective of the EU in building and regulating a strong internal market in health goods and services, and the rights of the individual patient relating to data concerning them.

¹ https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en- the EHDS Regulation is expected to enter into force in Spring 2025.

The EHDS Regulation and Health Data Protection fit for the digital age

The proposed EHDS Regulation has been developed to support the internal market as set out in Article 114 of the Treaty on the Functioning of the EU (TFEU); protect the interests of individuals in health data concerning them as set out in Article 16 TFEU; and at the same time promoting a high level of human protection across the EU and respecting Member State responsibility for the definition of their health policy and for the organisation and delivery of health services and medical care as provided for in Article 168 TFEU.

Central to the functioning of the EHDS is the capacity to collect, access and re-use health data. It therefore has to complement and enhance the General Data Protection Regulation (Regulation (EU)2016/679)², generally known as GDPR, ensuring that patients can exercise their rights, while at the same time valuable health data is freed up for use. Below we look at three key elements of the interaction between the EHDS Regulation and GDPR looking at patients' rights to access data, the new rules for data re-use and the rights of patients to opt-out of their data being shared for care or for research purposes.

The GDPR is the cornerstone of protection of personal data in the EU. It is considered by many as the world's strongest set of data protection rules, which enhance the rights of people to access information about themselves, take control of data concerning them and places limits on what organisations can do with personal data. With respect to patients' right to control data about them, the GDPR is not ideal, as the right to data portability that it creates is limited to data collected on the basis of consent.

Consent, however is rarely the legal base for data collection in healthcare, being usually based on the legal duty of the healthcare professional to collect data in order to provide safe healthcare. While GDPR opens the door for re-use of data, for instance for research under specific safeguards such as pseudonymisation or anonymisation, it has also created a fragmented EU landscape on access to data for re-use, as the GDPR requires each Member State set its own legal framework for such re-use.

Patients' rights to data access, portability and control

The EHDS seeks to address the challenges above by enhancing the GDPR, which remains in force and must be respected, by building on the rights created in the GDPR. From the patients' perspective it creates an absolute right of data portability – thus while under GDPR data was only portable if it was collected based on consent, and furthermore natural persons have the right to have the personal data transmitted directly from one controller to another only where technically feasible as GDPR does not impose an obligation to make this direct transmission technically feasible.



² [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)

What's next for data protection in healthcare in the EU?

The EHDS Regulation will however ensure that patients can always have their data electronically transmitted from one care provider to another or given themselves directly in electronic format free of charge.

Furthermore, Member States are required to establish electronic health data access services in order to make the exercise of rights by patients as easy as possible. A further feature of the EHDS Regulation is the absolute right of a patient to insert information into their health record. Previously, the right to add data was regulated at Member State level, meaning that the right to add to their health record did not exist for all patients, but when the EHDS Regulation enters into force all patients across the EU will have the right to add information into their electronic health record, albeit in a way that makes clear to a health professional that the data are patient added.

Access to data for re-use in health and life sciences research and for health systems planning and policy development.

Health data has huge potential to drive research and innovation; however, the privacy of individual data subjects must be protected. The GDPR left the balance between these two competing interests to be addressed in national law, creating a fragmented legal framework and making cross-border re-use of health data for research very difficult. The EHDS seeks to address this by creating a new legal base of re-use of data for research. Accordingly, researchers, industry or public institutions will have access to data in an anonymised format when the objective of the re-use can be achieved using data in this format - thus protecting the privacy of the individual.



Where anonymised data is not sufficient, the health data access bodies shall provide access to electronic health data in pseudonymised format, furthermore the re-use of health data must take place in a specially designed secure processing environment for specific purposes that benefit individuals and society.

The right to opt-out

Given that the EHDS Regulation will apply alongside the GDPR, patients have a right to control who may access their data and for what purposes it may be used. While the sharing of health data for care purposes between health professionals is generally seen as desirable by patients who want their care providers to have access to the relevant information to be able to treat them, in some cases patients may want to limit who can see their full care record. The EHDS Regulation therefore makes clear that Member States should be able to provide for an absolute right of a patient to opt-out from access to their personal electronic health data by anyone other than the original data controller. The right to such opt-out will be regulated at Member State level, this means some Member States may choose not to allow it, and some may allow it in a more limited way in which healthcare professionals may still access the data if to do so is necessary to protect the vital interests of the patient, noting that this term would be construed narrowly as set out in the GDPR.

With respect to opting-out of re-use of data for secondary purposes such as research or health system planning, the EHDS Regulation creates a right at EU level. This means that each Member State will have to set up a mechanism by which the patient can opt-out of their data being made available for secondary use. This right shall apply at any time and patients will not have to provide any reason. While the right to opt-out is provided at EU level, a Member State may provide for a mechanism at national level for a public sector body which has a mandate to carry out tasks on public health to use data including data from patients who have exercised the right to opt-out if the research in

question is on a matter of important public interest.

Is the EHDS Regulation enough to make Health Data Protection fit for the digital age?

With its capacity to strengthen the rights of patients to access and add to their health records and to have such records shared, and also creating mechanisms to ensure patient retain control of who may view their data for their care and who may access it for research, the EHDS goes a long way to creating a data protection regime which balances the rights of the individual with the needs of a strong EU internal market in digital health services.

However, legislative texts are not routinely read by patients, and indeed many health professionals will not have the interest or time to make themselves fully informed about the new rights and obligations the EHDS Regulation creates. In order for these rights to be understood and exercised, a significant investment will have to be made into educational support and advocacy to ensure that patients know what they can ask for and what impact of access to their health data or limiting access to it by others might have.

Recommendations:

► Build awareness among citizens

Individuals should be informed about their rights in an accessible manner through a range of communication channels. Such information should be provided in an engaging manner, in multiple languages used in a community and regularly reinforced through advocacy campaigns.

► Provide training and support for health professionals and support staff

Health professional and support staff must be well informed about citizens' rights and must have the capacity to respond to requests for access, to be able to provide assistance with data inclusion into records by patients and know how to help a patient exercise their right to opt-out. When the opt-out is for a particular category or categories of data for care, they must be able to explain the potential impact on future care in an unambiguous manner, while at the same time not limiting patients' control.

► Invest in agencies and human resources

Investing in human resources across healthcare institutions, government agencies, patient organisations to improve digital literacy, training and capacity building should not be underestimated in order to optimise the uptake of digital health technologies. Building and maintaining trust of all stakeholders involved is paramount but patients are the key as addressing their concerns regarding handing of their health data can make or break a delicate system that runs on data.