Data portability in the European Health Data Space: Benefits, Risks, and Challenges

Written by Florina Pop and Laura Grant

and Marina Koci

Part two of the series: Exploring the Proposal for a European Health Data Space

Read part one here

I. Introduction

At the heart of new European Union (EU) policy initiatives - such as the proposal for a **European Health Data Space** (EHDS) - is the empowerment of data subjects by enhancing their rights. The right to data portability under the General Data Protection Regulation (GDPR) allows data subjects more control over their own data and facilitates their ability to transfer/copy their data easily from one provider to another. A main focal point of the EHDS proposal is the fact that it builds on data portability under the GDPR, broadening its scope. This right and the challenges underlying the proposal are the focus of this *second* installation in our blog post series. This blog explains the right to data portability, highlighting the main practical benefits to patients, risks, and challenges the proposal will bring with respect to this right.

II. What is the right to data portability?

The GDPR defines the right to data portability in **Article 20(1),** stating that individuals have the right to receive their personal data in **a clear, easy way,** and **the right to send these data to another controller** without hindrance from the original controller.

The right to data portability correlates to the **right of access** under **Article 15 GDPR.** It helps data subjects not only to access their data, but also to manage and reuse data across applications of their preference. The right to data portability, under the GDPR, applies only when:

- Processing is based on either consent or contract;
- Processing is carried out automatically.

Data portability was viewed more as an economic right than a data protection right by the GDPR drafters since they believed it would promote competition among digital business and platform interoperability, thus the legal grounds of processing were limited.

III. What is the scope of data portability?

The types of data covered by GDPR's data portability right have been the subject of much debate. The Article 29 Working Party (now EDPB) has broadly interpreted **"data provided by the data subject"** to mean personal data knowingly provided to a controller plus observed data indirectly provided, which can be raw data e.g. location, activity logs, search history etc. This includes neither inferred data created by the controller, such as a user profile created based on raw data, medical diagnoses, or test results nor anonymised data.

Under the EHDS, the right data portability is found in **Article 3(8) EHDS** and linked to the **primary use** of health data, which we discussed in our first instalment of this blog series. The overall aim of expanding the scope of data portability in the EHDS is to allow patients to exchange and provide access to their primary health data processed by public or private

controllers between multiple healthcare providers (understood from Article 10(2)(o)(4) EHDS as pharmacies, hospitals, and other points of care). This will:

- Allow patients to make more informed choices;
- Prevent "lock-in" to one provider;
- Encourage competition in the healthcare sector

IV. Benefits and Implications

According to the definition of "electronic health data" and Recital 12, primary data portability in the EDHS, unlike the GDPR, also covers **inferred data**.

*What are the **benefits** of expanding the types of data that can be ported to include **inferred data**?*

Well, let us explain. A 2022 study by the European Parliament on the EHDS acknowledged these benefits. For example, a patient receives a diagnosis from a doctor in one hospital who analysed the patient's MRI/CT scan images. The scan images are the personal data knowingly provided by the patient and most likely in this case processed under consent. The diagnosis, however, is inferred data. Under the EHDS, the patient could then port the diagnosis (inferred data) to another healthcare provider for a second opinion. Similarly, if a patient who is a French national falls ill in the Netherlands and receives a diagnosis from a Dutch doctor, they would now be able to port that diagnosis (inferred data) back to their own doctor in France to continue the provision of their healthcare at home. Both these examples indicate how the expansion of the types of data included in the scope will facilitate informed choice and allow patients to receive better care.

*What are the **benefits** of expanding the **legal bases** of processing to data that can be ported?*

Based on Recital 12 EHDS, health data processed under any of the legal bases for processing in line with Article 9 GDPR will fall under the right to portability, as opposed to data processed only by consent or contract as in the GDPR. The benefits of expanding the scope of the legal bases for processing help minimise the limitations of the data portability right under the GDPR.

In terms of the practical benefits of expanding this element of the right, a 2019 research report by the University of Leiden (NL) demonstrated that the inability to port data that was processed not under consent or contract, but under another legal basis, may have negative consequences on the patient. For example, if a patient is in a coma, and medical tests are conducted, once better, that patient would not have the right to port that data which was processed to "protect the vital interest of the data subject" - not under consent or contract – to another healthcare provider if they so wished. However, under the EHDS, this is now a possibility. Enabling the expansion of this right will futureproof the legislation and ensure patients are able to port their data under nearly any circumstance.

*What are the **implications** of expanding the scope of the right to data portability?*

The expansion of this right, as highlighted by the EDPB/ EDPS in their Joint Opinion of July 2022, may create risks regarding the **data minimisation** and **purpose limitation** principles of the GDPR. This could be because allowing inferred data extends the scope of processing and because the EHDS will allow the processing of personal health data not based solely on contract or consent. This means that more data will be in circulation, which can potentially lead to organizations gathering and processing a larger amount of personal data than what is necessary for the purposes of the processing. For instance, a healthcare platform uses predictive analytics to infer a person's health conditions and potential health concerns based on their online activity (i.e. search history).

Accordingly, the data subject will be able to port these inferred data to another data controller, leading to the sharing of more information with various health providers.

V. Promoting interoperability

It's important to note that the right to data portability is closely related to the concept of **interoperability**, a key objective of the EHDS. Interoperability concerns the ability of different information systems to exchange and use data effectively and efficiently.

Interoperability

Source: European Data Protection Supervisor, 2022

When it comes to promoting data portability and interoperability, the GDPR and EHDS take different approaches. While the GDPR encourages data controllers to create interoperable formats that enable data portability, it does not require them to adopt or maintain technically compatible processing systems.

In contrast, the EHDS has set stricter requirements that are specifically focused on electronic health record (EHR) systems. These requirements are designed to promote interoperability and data portability, giving data subjects more control over their health data. Compared to the GDPR, the EHDS's requirements are much more stringent. By promoting interoperability and data portability in EHR systems, data subjects can more easily share and control their health data.

Manufacturers of medical devices and high-risk artificial intelligence systems declaring interoperability with EHR systems must comply with essential requirements on interoperability found in Annex II EHDS. Manufacturers should:

- Guarantee that EHR systems are developed in a manner enabling safe and secure processing;
- Implement the GDPR principles on data protection by design and by default;

In addition, manufacturers can voluntarily decide to label their products in compliance with EHR. This will need to be verified by the Member State market surveillance authorities.

Essentially, a lack of interoperability restricts data portability even within health systems, impeding health systems from providing effective treatment and patients to seek out competitive healthcare providers. This is precisely the problem that the EHDS aims to address by setting stricter requirements for EHR systems to promote interoperability and data portability.

VII. Conclusion

The EHDS and the GDPR are closely related, with the former seeking to increase the transparent processing of health data in a manner that is consistent with the GDPR's requirements. By enabling the easy exchange of health data, the EHDS empowers patients to take greater control over their health data, while also enabling healthcare providers to make more informed treatment decisions. Nonetheless, achieving interoperability can be a challenging task as it requires a high level of coordination, standardisation, and compatibility between different systems and technologies.

Interested in more?

If you're interested in following more on this topic, have a look at our upcoming Artificial Intelligence and Data Protection courses by clicking the button below:

The views expressed in this blog are those of the authors and not necessarily those of EIPA.