Make the European Health Data Space serve patients and research

European Digital Rights (EDRi) welcomes the proposal for a European Health Data Space ('EHDS') and its intention to provide for common rules and interoperable data standards that facilitate the sharing of health data where it is done in the medical interest of patients.

However, the EHDS proposal introduces a number of highly problematic new rules that would completely sabotage doctor-patient confidentiality and the reasonable privacy expectations EU citizens have when they confide in their doctor.

The proposal by the European Commission would make doctors and other medical professionals complicit in the forced commercialisation and monetisation of every aspect of our health without ever asking for our consent. It is no coincidence that a very similar law in Germany is currently being challenged before the country's constitutional court.[1]

Insurance companies, the pharmaceutical industry and, of course, Big Tech corporations like Google and Apple, only wait for an opportunity to get their hands on Europeans' health data. Apple has an extensive digital health offer[2] and, in 2020, Google paid over US$ 2 billion to acquire health device maker Fitbit in an attempt to enter the health data market.[3]

> *"Are Google or its subsidiary, DeepMind, private entities performing research in relation to health or care sector [...]? Could Facebook's 'Reality Lab', Microsoft's 'Health Futures', or Amazon's 'AWS for Health' be encompassed by these provisions?"*[4]

It is therefore paramount that EU member states and the European Parliament fix the Commission's proposal and bring it in line with data protection law, established principles and fundamental rights.

---

1 Gesellschaft für Freiheitsrechte: "GFF klagt gegen die Sammlung der Gesundheitsdaten von 73 Millionen gesetzlich Versicherten: Daten sind besser gegen Diebstahl zu sichern", 3 May 2022. Available at: https://freiheitsrechte.org/ueber-die-gff/presse/pressemitteilungen-der-gesellschaft-fur-freiheitsrechte/pm-gesundheitsdaten.

2 See the official Apple Health app that collects everything from your heart beat to your sleeping patterns and medication intake: https://www.apple.com/ios/health.

3 EFF: "Google-Fitbit Merger Would Cement Google's Data Empire", 7 April 2020. Available at: https://www.eff.org/deeplinks/2020/04/google-fitbit-merger-would-cement-googles-data-empire.

4 Dr. Petros Terzisln: "Compromises and Asymmetries in the European Health Data Space", European Journal of Health Law, 27 October 2022. Available at: https://brill.com/view/journals/ejhl/aop/article-10.1163-15718093-bja10099/article-10.1163-15718093-bja10099.xml.

1. Require the patient's consent for the onward sharing of health data

The EHDS proposal entirely fails to protect patients when it comes to the sharing and use of their personal health data. While it claims to give individuals more control over their private information, the EHDS proposal in fact does the opposite: it completely deprives them of that control. Under the rules proposed by the Commission, patients would have no say over the sharing and commercial exploitation of their data and would not even be informed about who receives it.

> *"Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the [European] Convention [of Human Rights]. It is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general."*[5]

As a result, the proposal blatantly undermines the most fundamental principles of privacy established by GDPR, namely that the collection and processing of health data requires the data subject's consent, with the exception of narrowly defined circumstances. What is more, the proposed EHDS overrides the long-established principle of doctor-patient confidentiality.

Instead of acknowledging and safeguarding the special protections afforded to health data by GDPR and the European Courts' highest jurisprudence, the EHDS proposes to legally compel doctors and hospitals to betray that confidentiality and share sensitive medical information with new government-run agencies in each EU member state. Those agencies would then in turn make that data available to unknown third parties, including for commercial use. Nowhere does the EHDS foresee to ask patients whether they agree to their incredibly intimate medical data being used that way.

An 'opt-out' regime as proposed by the Rapporteurs' draft report is not an adequate solution because it unduly puts the burden of knowledge, understanding and decision on patients, who would be subjected to such opt-out in most vulnerable situations of illness and other health problems. Instead, the burden of proof and the responsibility to gain the patients' trust must lie with the data users who wish to access people's sensitive health data.

FIX IT

Any onward sharing of health data with parties other than health care providers involved in a patients' treatment must remain voluntary. Any obligation to register such highly sensitive data in electronic health records is to be rejected.

5 European Court of Human Rights in the case of *I v Finland*, Strasbourg, 17 July 2008. Available at: https://hudoc.echr.coe.int/eng?i=001-87510.

2. Limit the definition of health data

The EHDS proposal defines "health data" as a broad range of 15 categories data that goes way beyond what is strictly speaking information about patients' health or medical care. In line with its attempt to strengthen the commercialisation of people's medical records, the proposal extends the definition of "health data" to remotely related personal information such as insurance status, professional status, education, lifestyle, wellness and behaviour.

According to Recital 39, "health data" may even include information about the "consumption of different substances, homelessness, health insurance, minimum income, professional status, behaviour", and encourages data users to "enrich" (read: extensive profiling without consent) the data with sensitive information from other sources such as wellness apps or wearables.

Such broad data combination permissions are gold for data-intensive industries like Big Tech to conquer and dominate the healthcare market and combine it with their growing dominance of the so-called Internet of Things (wearables, smart home devices, digital home assistants, sensors, etc.).

This overstretched definition of electronic health data is met with a basically limitless provision of *who* can request access to that health data: namely "any natural or legal person".

It's easy to see a Big Tech company being granted a data permit for accessing data from insurance companies as well as education and meditation applications in order to develop a personalised recommendation system for a 'healthy lifestyle'. That way, the EHDS proposal not only undermines the data protection guarantees provided to citizens by GDPR, it also allows Big Tech gatekeepers to easily circumvent their obligations under the Digital Markets Act that have been expressly designed to prevent the use of big data as a way to dominate new markets.

FIX IT

Limit the definition of "health data" to what is directly related to health and medical care. Other data about people's economic, social and professional life must not be defined as health data.

3. Make the permitted purposes for data use precise and legitimate

The EHDS proposal's list of permitted purposes of health data processing is too long and too vague: For example, the Commission proposes that the government-run 'health data access bodies' shall provide access to any third parties they see fit to ensure "high levels of quality and safety of healthcare and of medicinal products or medical devices" (Art. 34, 1a); for the "training, testing and evaluating of algorithms, including in medical devices, AI systems and digital health applications" (Art. 34, 1g); or even just to all kinds of public authorities "to carry out their tasks defined in their mandates" (Art. 34, 1b).

This incredibly broad list is incompatible with the GDPR's legal requirement of purpose limitation for the processing of personal data established and gives the health data access bodies almost unlimited discretion to provide access to people's health data without accountability or recourse for patients.

The EHDS proposal's list of *prohibited* purposes in Art. 35 is pretty much limited to use cases that imply direct harm to patients. It does little to protect people against commercial or other abuse of their sensitive health data. It appears to be the very purpose of the Regulation to create an EU-wide market for sensitive health data in view of a full commercialisation and monetisation of people's health by private actors (insurance companies, the pharmaceutical industry, Big Tech, and many others) – but without the patients' consent.

What is more, it remains unclear how to deal with purposes that appear on neither of the two lists. It would be conceptionally much better for the EHDS to entirely remove the list of *prohibited* purposes and instead only allow purposes that are expressly mentioned in Art. 34.

FIX IT

The list of permitted purposes must be much more precise and limit the access to data to non-commercial academic researchers to produce non-proprietary research that is in the public interest. The list of *prohibited* purposes must be removed to avoid inconsistencies.

4. Data security must be top priority

Storing sensitive health data of over 500 million EU citizens in centralised data pools would attract the most sophisticated cybercriminals. The sheer amount and value of this data would turn health data access bodies into prime targets for malicious hacking by criminal and nation state attackers. Already today, there are regular incidents of theft and accidental exposure of large amounts of health data from hospitals, private insurance companies and health app providers. Mandating the collection of all this data in centralised databases will make the situation much more dangerous.

The EHDS should therefore clarify that data requested for secondary use be only transferred from data holders to a health data access body "upon request" and based on a specific research project approved by it. Such an approach puts safety first and enables health data access bodies to directly apply procedures such as data minimisation, differential privacy and, where appropriate, synthetic data creation before exposing it in a central data storage. Once the research project has been terminated, access bodies should be obliged to delete any related health data they still hold.

In addition, any health data stored by access bodies with the consent of patients must adhere to the highest operational and technical security standards as prescribed by GDPR, NIS-2 and related security certification mechanisms. That includes encryption and limitations to the transfer of health data outside the EU. Pseudonymisation and anonymisation are not enough: health data is so specific that re-identification can be trivial.[6] Often a person's social media or financial history, both widely available on today's data markets, is sufficient to identify medical events that can easily lead to re-identifying supposedly pseudonymised or even anonymised datasets. In addition, access bodies and data users for secondary use should be liable for any involuntary theft, re-identification or exposure of personal data. The EHDS should also foresee monetary compensation for patients in such cases.

FIX IT

The EHDS must impose strict security standards on health data access bodies and data users for secondary use. It should include a clear liability regime that holds those actors accountable for the misuse of health data and limit the transfer of data outside the EU in line with GDPR requirements.

6 Prof. Dr. Dominique Schröder: "Sachverständigengutachten zum Schutz medizinischer Daten", Chair for Applied Cryptography, University of Erlangen-Nürnberg, 25 April 2022. Available at https://freiheitsrechte.org/uploads/documents/Freiheit-im-digitalen-Zeitalter/Gesundheitsdaten/2022-04-25-Gutachten_Schroeder-Gesundheitsdaten-Gesellschaft_fuer_Freiheitsrechte.pdf.

Contact us

For any questions and to obtain more detailed information about how to improve the European Health Data Space, please contact

Jan Penfrat, Senior Policy Advisor
Email: jan.penfrat@edri.org
Phone: +32 2 274 25 70