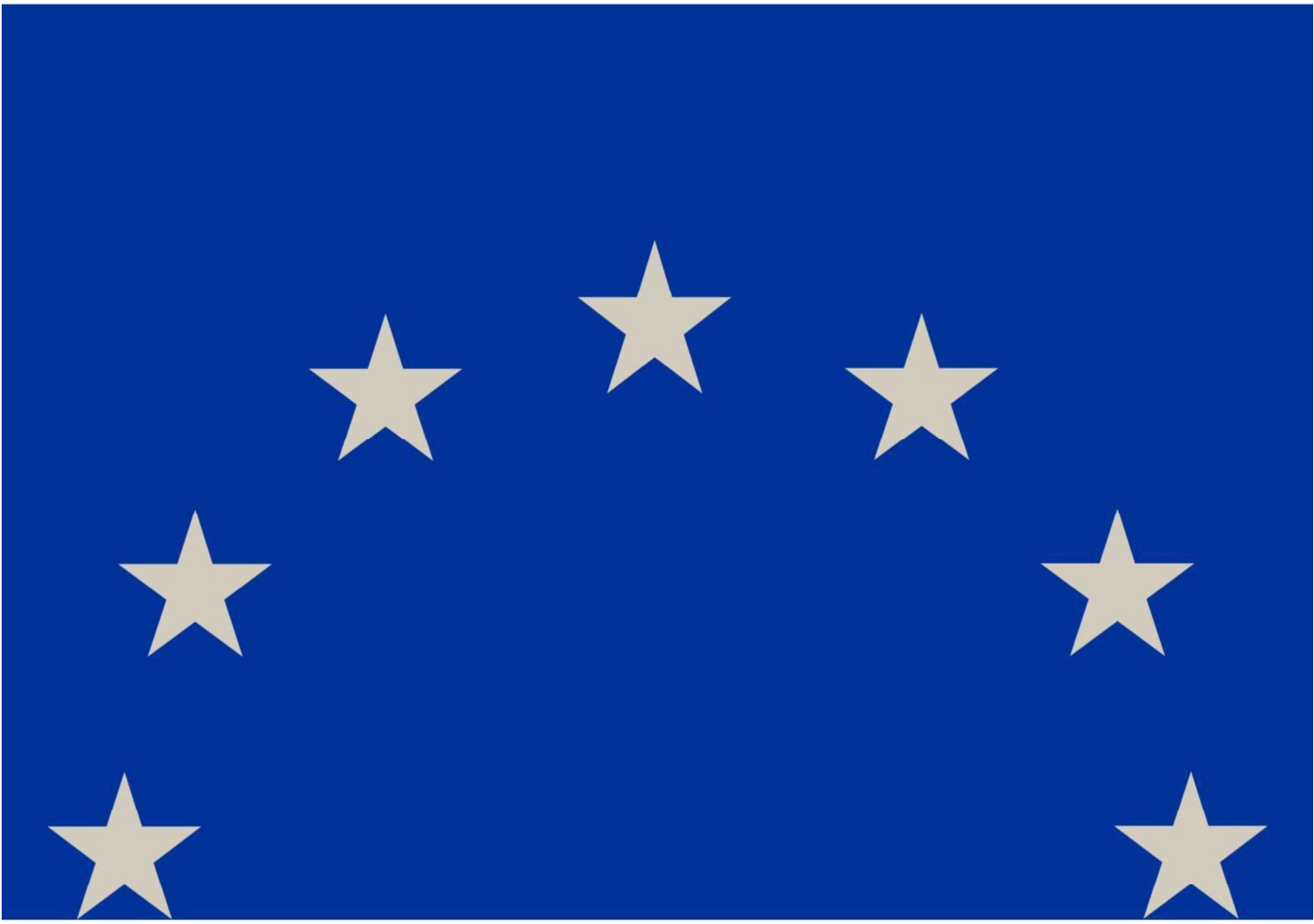
European Commission

DG SANTE
Unit C.1 – Digital Health

Frequently Asked Questions on the European Health Data Space

Last updated 26th of March 2026



Frequently Asked Questions on the European Health Data Space

Last updated 26 March 2026

Contents

Introduction

This document provides answers to frequently asked questions regarding the European Health Data Space (EHDS) Regulation (EU) 2025/327.

Any views expressed in this document are the preliminary views of the European Commission services and may not under any circumstances be regarded as stating an official position of the European Commission. The replies to the frequently asked questions do not extend or restrict in any way the rights and obligations deriving from applicable legislation nor introduce any additional requirements. The expressed views are not authoritative and cannot prejudge any future actions the European Commission may take, including potential positions before the Court of Justice of the European Union. Only the Court of Justice of the European Union is competent to authoritatively interpret EU law.

This is a living document that may be updated in the future. It complements other information related to the European Health Data Space Regulation. Please contact us if you have a question that is not covered. We will try to get back to you as quickly as possible.

Document last updated 26 March 2026.

Version	Date	Changes made
1.1	26/03/2026	Fixed typos and cross-references throughout. Expanded questions 22 and 55, 56. Added questions 24, 40, 48, 66, 67.
1.0	05/03/2025	-

General

1. What is the aim of the EHDS Regulation and its addresses?

The EHDS Regulation has three main parts, each with different addressees (see Article 1(2) of the EHDS Regulation):

Chapter II on primary use of personal electronic health data provides additional rights to patients compared to the General Data Protection Regulation (GDPR, Regulation (EU) 2016/679)[1] in relation with the use of those data for the provision of healthcare, also known as primary use. It sets out the technical infrastructure necessary for the implementation of primary use. Member States will have to ensure that the required infrastructure on their level is in place and that healthcare providers are connected to it. Chapter III on Electronic Health Record (EHR) systems is addressed to manufacturers and other economic operators who make EHR systems available on the market. It provides for requirements on such systems regarding interoperability and logging capabilities. It also sets up mechanisms for market surveillance of EHR systems, with provisions on the market surveillance authorities to be designated by the Member States and the activities of these authorities.

Chapter IV on secondary use of electronic health data is addressed to health data holders and users. It provides for obligations on health data holders to make those data available and frames how health data users can use such data. It provides for health data access bodies (HDABs) as well as the necessary infrastructure for the implementation of secondary use.

The remaining chapters deal with governance, for example setting up the EHDS Board, international aspects, and other cross-cutting topics.

Sources: Article 1, recital 1

2. Material scope – what is in, what is out?

On the definition of the material scope, see Article 1 of the EHDS Regulation, especially paragraphs:

(1) – this refers explicitly to *electronic* health data. Data that is not in a digital form is not in the scope of the Regulation.

[1] 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) (Text with EEA relevance).

(7) – this clarifies that legislation laying down disclosure obligations for certain health data in the public interest is not affected. This makes sure that for example notifiable diseases reporting and reporting of suspected adverse events in pharmacovigilance are not affected.

(9)(a) – this repeats that activities that are outside the scope of EU law are excluded from the scope of the Regulation (see Article 4(2) TEU). This means for example that activities for national security are excluded.

(9)(b) – this clarifies that the EHDS Regulation does not create an empowerment for such law-enforcement authorities to obtain health data. An example would be public prosecutors needing to obtain DNA samples to match against evidence found at a crime scene – the prosecutors need to use their investigate powers given to them by law to obtain that data and cannot use the EHDS for that purpose.

Sources: Article 1, recital 63

3. What is the timeline for the EHDS Regulation to become applicable?

The EHDS Regulation was published in the Official Journal on 5 March 2025 and entered into force 20 days later. However, it will start to apply in stages:

- Key provisions of Chapters II (on primary use) and III (on EHR systems) will apply four years after entry into force, i.e. from 26 March 2029, for the first group of priority categories (patient summaries, electronic prescriptions, electronic dispensations) and six years, i.e. from 26 March 2031, for the remaining priority categories (medical imaging studies, medical test results, discharge reports).
- Chapter IV on secondary use will apply four years after entry into force for most of the data categories listed in Article 51, so from 26 March 2029. For some categories, such as genetic data, it will apply six years after entry into force, so from 26 March 2031 (see also question 33 below). Article 75(5) of the EHDS Regulation on the possibility for non-EU countries to become authorised participants in HealthData@EU will apply ten years after entry into force, i.e. from 26 March 2035.

In practical terms:

As a patient, you will be able to use the health data access services and exercise your primary use rights from 26 March 2029 for the first group of priority categories listed under Article 14(1) of the EHDS Regulation (patient summaries, electronic prescriptions, electronic dispensations) and from 26 March 2031 for the remaining categories.

As a manufacturer of EHR systems, from 26 March 2029, you will only be allowed to place on the market EHR systems that comply with the common specifications for the harmonised components of systems

processing the first group of priority categories, and from 26 March 2031 for systems processing the remaining categories.

As a health data holder, you will have to submit descriptions of the datasets you hold to the relevant health data access bodies (HDAB) by 26 March 2029 or 2031, depending on which of the Article 51 categories (see question 33 below) each dataset falls into. By the same date, you may be required to make data available to the HDAB following a data permit / request decision.

As a health data user, you will be able to submit permit applications to HDABs and requests for most of the data categories in Article 51 by 26 March 2029. Two years later, you will also be able to do so for the remaining categories (data on factors impacting on health, including socio-economic, environmental and behavioural determinants of health; human genetic, epigenomic and genomic data; other human molecular data such as proteomic, transcriptomic, metabolomic, lipidomic and other -omic data; data from clinical trials, studies and investigations; research data).

Member States will have to set up their digital health authorities and designate their national contact points by 26 March 2027. By 26 March 2029, they will need to ensure that the services at Member State level for primary use are up and running for the first group of priority categories listed under Article 14(1) of the EHDS Regulation (patient summary, electronic prescriptions, electronic dispensations). By 26 March 2031, they will have to extend these services to the remaining priority categories.

For secondary use their health data access bodies (HDABs) must be ready to receive applications, as well as be connected to HealthData@EU by 26 March 2029 or 2031, depending on which of the Article 51 categories each dataset falls into (see question 33 below).

Other provisions, such as those on governance and the setup of the EHDS Board will apply two years after entry into force, thus by 26 March 2027.

Sources: Article 105; recital 115

4. What is the Commission doing to prepare for application? When can we expect to see implementing acts adopted?

While the transition periods may seem long at first sight, there is a lot of work to do to get ready for all stakeholders involved – be that Member States, healthcare providers, or the Commission itself.

The EHDS Regulation sets out the framework for how the EHDS will operate. But there are plenty of technical details that will be set out in delegated and implementing acts – ranging from the technical specifications of the European electronic health record exchange format and detailed requirements for EHR systems manufacturers when they register their systems, to the security measures for secure

processing environments. In addition, once those technical details have been set out, the systems will need to be built, tested, and deployed.

That is why the EHDS Regulation includes a deadline of 26 March 2027 for the Commission to adopt key implementing acts: two years to set out the detailed blueprints, and then two more years to build, test, and deploy them before key parts of the EHDS Regulation become appliable four years after entry into force.

The key implementing acts with this deadline are mentioned in:

- Article 13(4) on data quality requirements for primary use;
- Article 15(1) on the technical specifications for the EEHRxF;
- Article 23(4) on MyHealth@EU;
- Article 36(1) on common specifications for the harmonised components of EHR systems;
- Article 70 on templates for data access applications, permits and requests;
- Article 73(5) on requirements for secure processing environments;
- Article 75(12) on HealthData@EU;
- Article 77(4) on the requirements for dataset descriptions;
- Article 78(6) on the data quality and utility label.

Implementing acts will go through the usual comitology procedures involving Member States as well as the required public consultations, while delegated acts adopted by the Commission will be subject to a period during which the European Parliament and the Council may object to the delegated act, in accordance with Article 290 TFEU. There are several empowerments for delegated acts, e.g. in Article 49(4) for supplementing the EHDS Regulation with a list of required data to be entered into the EU database for registration of EHR systems and wellness applications by the manufacturers of those systems and applications.

Sources: Article 105; recital 115, EHDS Committee in Comitology Register

5. What is the Commission doing to support Member States as well as healthcare providers and other stakeholders in preparing to apply the EHDS Regulation?

The Commission is funding many projects and joint actions in preparation for the implementation of the EHDS Regulation. Some examples are:

Xt-EHR – working on implementation guides, technical specifications, and a conformity assessment framework for the adoption of the European electronic health record exchange format (EEHRxF) and for the implementation of security and logging mechanisms.

EHDS2 Pilot Project – piloting connecting data platforms in a network infrastructure and developing services supporting the user journey for research projects using health data from various EU Member States.

TEHDAS 2 – developing guidelines and technical specifications for implementation of secondary use.

QUANTUM – developing criteria for a data quality and utility label.

Primary Use (Chapter II)

For patients

6. Over which kinds of data can I exercise my EHDS rights as a patient?

Under the EHDS Regulation, you will have an additional right compared to the GDPR to access, control, and share specific categories of your personal electronic health data. You will be able to exercise these rights using an online service. These additional rights apply to the following categories of personal electronic health data listed under Article 14(1) of the EHDS Regulation, collectively called 'the priority categories'. These rights will start to apply in two phases:

First phase:

1. patient summaries (an extensive set of key clinical data including health problems, medication, vaccinations, treatment plans, etc);
2. electronic prescriptions;
3. electronic dispensations (information that a prescription has been used).

Added in second phase:

4. medical imaging studies and related imaging reports;
5. medical test results, including laboratory and other diagnostic results and related reports;
6. discharge reports.

You will be able to exercise these additional rights over the first three categories by 26 March 2029 (first phase) and by 26 March 2031 over the last three categories (second phase) (see question 3).

These rights apply to these data categories when such data are processed electronically (see question 2). For example, a discharge report that exists only on paper would be not be covered. The EHDS Regulation creates no obligation to digitise paper documents. These rights are about giving patients better insight into and control over such data when they are processed electronically.

These rights also cover historical data, as long as it is in digital form, – they are not limited to documents generated after these rights start to apply.

Sources: Articles 14 and 105; recitals 9, 11, and 115.

7. As a patient, how will I exercise these rights, what tools will I have?

You will be able to exercise your rights under the EHDS Regulation through secure health data access services, free of charge (see Article 4 of the EHDS Regulation). These online services will provide you with a dashboard allowing you for example to : (i) access (view) your own data, (ii) see who has accessed it, (iii) report inaccuracies, (iv) restrict access to data, and (v) manage your proxy authorisations (on proxy services, see also question 15).

Authentication for accessing these services will use secure electronic identification methods (eIDs), recognised under Article 6 of the eIDAS Regulation 910/2014[2]. In many cases, national eIDs will qualify as secure methods (see also question 19 below).

An additional design requirement is that these services must be easy to use, for example for people with disabilities, vulnerable groups or people with low digital literacy.

Sources: Articles 4, 6, 8, 9, 16; recital 20

8. How will the right of access work for me as a patient? Are there exceptions?

The EHDS Regulation will grant you the right to immediate access to the priority categories of your electronic health data through a secure health data access service (see also question 7). This access will also always be free of charge for you.

Patients can look at their data in the access service, in practice using a form of a dashboard. As a patient, you will be able to download the data as well.

However, there are two restrictions to this right of access:

First, Article 3(1) of the EHDS Regulation acknowledges that due to the need for technological practicability, there might be slight delays in data availability in some cases. For example, there may be a short time lag between for example the issuing of a laboratory report is issued and when it shows up in your dashboard in the health data access service.

Secondly, immediate access to certain information could be harmful in some cases. That is why Member States may, where necessary for the protection of the patient, impose rules on a delay so that certain information is shown in the dashboard only *after* a treating health professional has explained the information and its consequences to the patient.

[2] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

For example, think about laboratory results confirming that a patient has a life-threatening health condition. To protect the patient, it may be appropriate for them to learn about this during a consultation with their treating health professional, who can then explain the diagnosis, prognosis, and treatment options. After this explanation, the information would then also become visible (and downloadable) in the health data access service like any other health data in the priority categories.

Sources: Articles 3, 4, and 9; recitals 9 to 11, 25

9. As a patient, can I add information in the electronic health data access service?

Yes, under Article 5 of the EHDS Regulation, you have the right to add information to your electronic health records via the health data access service, including data from an interoperable wellness application (see question 30).

The EHDS Regulation does not list data elements that can be inserted. However, the intention is to enable patients to complement data in the priority data categories as referred to in Article 14(1) of the EHDS Regulation.

Any information added by the patient will be clearly distinguished from information entered by health professionals.

This right only applies to *adding* information. Information provided by health professionals cannot be *changed (or deleted)* (for correcting errors in information, please see question 10 below).

Sources: Article 5; recital 12

10. As a patient, if I see incorrect information in the electronic health data access service, how can I get it corrected?

As a patient, if you see incorrect information in the electronic health data access service, you will be able to request that it be rectified through the functionalities provided by the health data access services. Such requests will then be forwarded to the original source of the contested data (that is to say, the controller for the processing operations from which they originate) who will assess it and correct the data if needed.

However, it is important to note that you will not be able to directly change yourself data that you believe to be incorrect, e.g. in a patient summary.

Sources: Article 6, recital 13

11. How will the EHDS Regulation improve data portability for me as a patient?

Article 7 of the EHDS Regulation will significantly improve the portability of personal electronic health data for patients.

You will have the right to receive and share your electronic health data in the European electronic health record exchange format (EEHRxF – see also question 16 below). This will facilitate seamless data exchange between healthcare providers across the EU. This means that healthcare providers must be able to export and import data in this format. However, this does not affect which formats they use internally.

This complements the right to data portability under the GDPR, but has important differences:

1. Data portability under the GDPR only applies to data processed based on consent or contract. Portability under Article 7 of the EHDS Regulation applies regardless of the legal basis of the processing.
2. Data portability under the GDPR only applies to data provided by a data subject to a controller, including observed data, but not inferred data. Portability under Article 7 of the EHDS Regulation applies regardless of whether data was provided ('patient reports pain in left knee'), observed ('x-ray image of the knee'), or inferred ('the problem with the knee is X').
3. Under the GDPR, the data subject has the right to receive and share data in a commonly used format. There is, however, no requirement for the controllers from and to whom the data subject imports/exports data to support the same format. The EHDS Regulation creates an obligation on both parties to support export/import of data in the EEHRxF (see also question 16 below).

To exercise the right for data portability you do not need to send the data yourself. Instead, your data can be transmitted from its source to the health professional treating you or to the social security or reimbursement services sector. In practice, this works in such a way that the health professional can issue a request for your data, and the data will be provided by the data source (apart from any restricted parts, see question 12 below). Alternatively, you can download your data and transmit it to the healthcare provider of your choice yourself.

Sources: Article 7, recital 15

12. How will the right to restrict access work for patients? What is the effect on health professionals?

The right to restrict access allows patients to limit who can see all or certain parts of their electronic health data in the priority categories listed under Article 14(1) of the EHDS Regulation that can be shared.

In case of partial restriction, any data that have not been restricted will remain available via the secure health data access services set up under the EHDS.

Data that has been restricted by the patient will not be accessible to health professionals using the EHDS access services, and no indication of the restriction (such as a notification of hidden information) will be visible to them. This is a right granted directly by Article 8 of the EHDS Regulation.

However, there will be an exception: in critical situations, health professionals can trigger a 'breaking the glass' mechanism – for example when an unconscious patient arrives in an emergency room, the health professionals treating them could use this exception to make sure that they have all available information at their disposal to provide the best care.

Sources: Article 8, recital 17

13. How will the right to opt out in primary use work?

Article 10 of the EHDS Regulation gives Member States the option to allow patients to opt out of the exchanges set up under the EHDS Regulation for primary use. *If* a Member State chooses to do so (by means of national law), patients will thus have the right to withdraw *completely* from the data exchanges set up *by the EHDS* for primary use. As a result, people who have opted out will, be unable to access their own electronic health data through the electronic health data access services set up under the EHDS.

Additionally, health professionals would be unable to access the patient's health data, such as retrieving a patient summary, through the EHDS health professional access service. For example, a health professional treating a new patient will not be able to use the health professional access service to obtain the patient summary, and lab test results of someone who has opted out. However, Member States can also establish exceptions similar to the 'breaking the glass' scenario that can apply to this right.

Please note also that when people exercise their right to opt out from primary use under the EHDS Regulation, this does not affect the initial registration of data by the treating healthcare provider – for example, a hospital would keep the same documentation of an MRI scan, but it would not be able to share it *through the services set up by the EHDS.* Patients who use this opt-out would find themselves in a similar situation as before the EHDS.

The right to opt out in primary use is separate from the right to opt out in secondary use. When a patient has opted out in primary use, that does not mean that they are automatically opted out in secondary use, and vice versa (see question 46 below).

Sources: Article 10, recital 18

14. What is the difference between the right to restrict access and the right to opt out in primary use?

The right to restrict means that patients will be able to limit who sees specific parts of their electronic health data in the priority categories listed under Article 14(1) of the EHDS Regulation, so that only some data is accessible. Patients can also restrict health professionals' access to all their data in the health data access services set up by the EHDS. However, a 'breaking the glass' scenario allowing access to a patient's restricted data will be possible in emergencies. Other data that has not been restricted will remain available via the health data access services set up under the EHDS. This is a right granted directly by the EHDS Regulation.

These restrictions do not impact other rights of natural persons under the EHDS Regulation. For instance, patients themselves can still exercise the right to access their electronic health data in the health data access services set up by the EHDS, including the restricted parts.

In contrast, the right to opt out in primary use is an option that Member States *may choose* to offer through national legislation. If they chose to do so, people will have the right to withdraw their electronic health data completely from the data exchanges *set up by the EHDS for primary use*. If patients choose to exercise this right, all their data would be excluded from the EHDS data exchanges for primary use, meaning for example that health professionals or patients themselves cannot access their patient summary or other data through the health data access service provided by the EHDS, regardless of whether this were to take place nationally or in a cross-border setting. Please note that this does not affect the registration and availability of data in local systems – the health professionals that provided treatment to you will still be able to register information on that treatment in their local system and access it.

Sources: Articles 8 and 10, recital 17, 18

15. How will the proxy services work?

Proxy services under the EHDS Regulation will allow another person to act on behalf of a patient regarding access to their electronic health data. The proxy services deal with two main situations:

1. A patient authorises somebody else to act on their behalf, for example someone authorising their spouse to access their records.
2. A legal guardian acts on behalf of a child. The most common example here is parents acting for their minor children. In this case, the relevant Member State's rules on guardianship apply – the legal guardian's access could vary, for example, depending on whether the child is a toddler or a teenager.

The use of proxy services will be free of charge. It must be possible to submit authorisations online or on paper.

Sources: Article 4; recitals 20, 21

16. What is the European electronic health record exchange format and what is its purpose?

One of the main obstacles to interoperability and seamless exchange of health information for providing treatment is the use of different and often incompatible file formats for data – for example, hospitals are often technically not able to import reports from other hospitals into their own systems. This is a problem particularly in cross-border situations but is also common within the same Member State.

The European electronic health record exchange format (EEHRxF) is designed to address the challenges of interoperability and enable the seamless exchange of health information for the priority categories of personal electronic health data listed under Article 14(1) of the EHDS Regulation across different healthcare systems within the EU. It provides a common European format for describing the priority categories (see question 6 above). EHR systems (see question 22 below) will have to be able to import and export data in this format. This will be an important step forward for the interoperability of electronic health data. In simple words: the EEHRxF will be a common language that EHR systems must be able to speak to one another.

The detailed specifications will be set out by the Commission in an implementing act, which must be adopted within two years of entry into force of the EHDS Regulation, i.e. by 26 March 2027 (see Article 15 of the EHDS Regulation and question 4).

The specifications are expected to build on the work of the XT-EHR Joint Action , which in turn builds on the results of previous EU-funded projects such as XpanDH, x-eHealth, and epSOS, as well as on Commission Recommendation (EU) 2019/243 on a European Electronic Health Record exchange format (see Q5).

Sources: Article 15; recital 26

17. What is MyHealth@EU?

MyHealth@EU is the cross-border infrastructure supporting the primary use parts of the EHDS.

It is through this infrastructure that, for example, patient summaries will be exchanged across borders. The Commission will provide central services to the Member States. Member States' national contact points will connect to this infrastructure. The actual exchanges of electronic health data will be point-to-point: for example, if you seek medical care abroad in Member State B, the local healthcare provider will be able to consult your patient summary. This summary will be obtained from Member State B's national

contact point, which requested it via MyHealth@EU from Member State A, where you live and consult doctors.

MyHealth@EU does not include a central repository of electronic health data – it only supports the point-to-point exchanges between national contact points.

MyHealth@EU will be a development of the existing infrastructure of the same name that already supports voluntary exchanges of patient summaries, electronic prescriptions and electronic dispensations between several Member States. The difference is that connecting to MyHealth@EU under the EHDS will become mandatory for Member States and the scope of the data to be exchanged will increase (see the priority categories of personal electronic health data listed under Article 14(1) of the EHDS Regulation and question 6).

Sources: Articles 23 and 24; recitals 33 to 35

For health professionals

18. As a health professional, what is the benefit of the health professional access service for me?

As a health professional, the health professional access service referred to in Article 12 of the EHDS Regulation will provide you with free-of-charge access to the priority categories of personal electronic health data listed under Article 14(1) of the EHDS Regulation relating to the patients you are treating. This will improve the information available to you, in order to give your patients the best treatment. The health professional access service and the patient-facing access services are two sides of the same coin.

In the course of treating a patient, healthcare providers should access only the data strictly necessary and justified for a given health service, according to the data minimisation principle of the GDPR. The Member State where you work will set out detailed rules on this access – for example, to distinguish between the access rights of different categories or specialisations of health professionals.

In cross-border situations, the rules of the Member State of treatment apply. If, for example, you are a nurse and the Member State where you provide treatment has different access rights for nurses compared with doctors, you will have the same access rights for cross-border cases as for a 'local' patient.

Sources: Article 12; recital 19

19. How will patients and health professionals authenticate themselves to the access services?

Patients will be able to authenticate themselves to the health data access services using reliable electronic identification means, such as those compliant with the European Digital Identity Framework, i.e. the EU Digital Identity Wallets and national electronic identification means recognised under Article 6 of Regulation 910/2014[3] (see Article 16 EHDS Regulation and question 7). Commonly these will be the same eIDs as the ones accepted by other public and private online services.

Health professionals can use the same kind of identification means compliant with the European digital identity framework. Many Member States already provide national electronic identification means to their licensed health professionals. They could continue to be used as long as they are compliant with common specifications to be adopted by implementing acts under the Article 36 of the EHDS Regulation. At the same time, health professional access services provided by public-sector bodies or by private parties (except small and medium-sized enterprises) will always have to accept European digital identity wallets where the requirements of Article 5f(1) and (2) of Regulation 910/2014 are met.

Additional steps beyond basic electronic user identification are needed to verify the health professional's professional qualifications. The reason for this is that electronic identification means are commonly focused on basic identification – they provide assurance that the person using them is who they claim they are. In simple terms, they prove that 'this person is indeed Jane Doe'. However, the information 'Jane Doe is a registered nurse working in the maternity ward of Capital City University Hospital' is (usually) not part of the attributes that they prove. More advanced identification mechanisms, such as EU digital identity wallets, will also enable proof of qualification to be provided or sharing of other attributes, and Member States can consider using this functionality.

Sources: Articles 12 and 16; recital 29

For Member States' authorities

20. What will the tasks of the Digital Health Authorities be?

The Digital Health Authorities will have the tasks listed in Article 19 of the EHDS Regulation. They will be responsible for organising the implementation of the EHDS framework related to primary use in their Member State – for example ensuring that the relevant technical solutions are put in place for implementing the additional rights for patients compared to the GDPR, and providing relevant information to patients, health professionals and healthcare providers.

[3] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

Sources: Article 19; recital 30

21. Who will set up the health data access service and health professional access service?

The EHDS Regulation places the responsibility on Member States to ensure that health data access services and health professional access services are available.

Under Article 168(7) TFEU, Member States are entitled to organise their healthcare systems as they see fit, but they are responsible for the results – what matters is that the services are operational and accessible. The way services are provided, e.g. whether directly provided by the state or by other organisations entrusted with such tasks in the national systems is therefore left to for Member States to decide. Access services should be linked to proxy services (see question 15 above).

Sources: Articles 4 and 12; recitals 20, 21

Requirements for EHR systems and wellness apps (Chapter III)

For manufacturers/importers/distributors of EHR systems

22. Which products/services exactly count as EHR systems?

Electronic health record (EHR) systems are defined as (see Article 2(2) point (k) EHDS Regulation) 'any system whereby the software, or a combination of the hardware and the software of that system, allows personal electronic health data that belong to the priority categories of personal electronic health data established under this Regulation to be stored, intermediated, exported, imported, converted, edited or viewed, and intended by the manufacturer to be used by healthcare providers when providing patient care or by patients when accessing their electronic health data.'

This definition has the following elements:

- EHR systems can be a combination of hardware and software or just software: an EHR system can be part of a physical device or self-standing software;
- They allow the storage, intermediation, export, import, conversion, editing, or viewing of priority categories of personal electronic health data listed under Article 14(1) of the EHDS Regulation (see question 6 above): a system that only processes other kinds of data (such as a system for patients to book appointments) is not an EHR system;
- Systems do not need to provide all of storage, intermediation, export, import, conversion, editing, or viewing functionalities together to be considered as an EHR system;
- They are intended by their manufacturer to be used:
    - by healthcare providers when treating patients: the classic example is systems used by clinicians for recording notes, test results etc. up to a patient management system; or
    - by patients when accessing their electronic health data: for example, an app that connects to the electronic health data access service for patients will count as an EHR system. On the other hand, a smartwatch that allows users to view their health data would not qualify as an EHR system because it operates outside the context of healthcare provision, i.e. specifically, outside settings where a *patient* is actively seeking or receiving medical care.

This definition is deliberately broad: to ensure interoperability throughout the chain of connected systems. It not only applies to systems that aggregate information, like hospital information systems, but also to the systems 'feeding' them. Article 25(2) of the EHDS Regulation and recital 38 clarify that when general purpose software is used for these general purposes, it does not count as an EHR system: standard text processing software can be used to edit any kind of textual information, including for

example patient summaries, but it is not specifically intended by the manufacturer for use in treating patient care[4] and so does not count as an EHR system.

Products may have parts that fall under different certification systems such as under the Medical Devices Regulation[5], the Artificial Intelligence Act[6], the Cyber Resilience Act[7] or the EHDS Regulation. In such case, each part of the product needs to comply with the applicable certification framework as applicable. Please note that the rules under Regulation (EU) 2024/1689 (AI Act) in relation to the Medical Devices Regulation and In-Vitro Devices Regulation are currently under revision[8], to ensure a single application and assessment when AI is embedded in those types of devices. As a consequence, these provisions might need to be adapted following that revision.

Please find some illustrative examples below:

In scope:

- An information system used in a pharmacy to read electronic prescriptions, process dispensations at the pharmacy and to issue an electronic dispensation.
- A patient information portal allowing a patient to access electronically health data documents produced in the provision of healthcare services that are included in the priority categories of personal electronic health data listed under Article 14(1) of the EHDS Regulation, e.g. electronic prescriptions, medical images and reports such as X-ray or MRI scans, laboratory results of blood or urine tests.

[4] This mirrors a similar exclusion in recital 19 of the Medical Device Regulation 2017/745: clinical decision support software is considered a medical device, but if a health professional uses general purpose software such as spreadsheet software to create a spreadsheet template calculating dosage recommendations, that does not make the (generic) spreadsheet software itself a clinical decision support software.

[5] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, OJ L 117, 5.5.2017.

[6] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828, OJ L, 2024/1689, 12.7.2024.

[7] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828, OJ L, 2024/2847, 20.11.2024.

[8] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulations (EU) 2017/745 and (EU) 2017/746 as regards simplifying and reducing the burden of the rules on medical devices and in vitro diagnostic medical devices, and amending Regulation (EU) 2022/123 as regards the support of the European Medicines Agency for the expert panels on medical devices and Regulation (EU) 2024/1689 as regards the list of Union harmonisation legislation referred to in its Annex I COM/2025/1023 final.

- A system converting the output of legacy EHR systems into the European electronic health record exchange format (EEHRxF).

Out of scope:

- Scheduling system for appointments with a general practitioner;
- Administrative billing system, unless it processes diagnosis, medication or other patient data from priority categories of personal electronic health data listed under Article 14(1) of the EHDS Regulation for preparing the bills;
- A wellness application processing non-medical data, e.g. sleep information or measuring intensity and duration of physical activity.
- A smart (digital) thermometer connected to a smartphone app, used by individuals to take their temperature.

Sources: Articles 2(2), point (k) and 25(2); recital 38

23. What are the specific requirements that EHR systems will have to comply with?

To be placed on the market or put into service in the EU, EHR systems must contain the two harmonised software[9] components, namely:

- the interoperability component, and
- the logging component.

These 'components' describe capabilities of EHR systems.

The interoperability component provides the capability to import/export data that falls under the priority of personal electronic health data listed under Article 14(1) of the EHDS Regulation (see question 6) in the European electronic health record exchange format (EEHRxF).There is no requirement for EHR systems to use the format internally.

The logging component provides the capability to generate logs that can be used in the health data access service to provide transparency on data access (see question 7 above).

The detailed specifications will be set out by the Commission in implementing acts to be adopted by 26 March 2027 (see question 4).

[9] While EHR systems as a whole can have physical/hardware and software parts, these two components will logically always be software.

Manufacturers will be obliged to test these components in automated testing environments (see question 26 below) before placing EHR systems on the market.

Please note that while these will be the requirements for placing EHR systems on the market, Member States may also maintain or lay down specific rules for the procurement or financing of, or reimbursement of EHR systems (see Article 29 of the EHDS Regulation for the details). The requirements of the EHDS Regulation only cover the two harmonised components. Please check Member State requirements on other parts of EHR systems.

Sources: Articles 2(2) points (m) to (o), 25, 26, 29; recitals 36, 39

24. I produce medical devices / in-vitro medical devices / high-risk AI systems that are interoperable with EHR Systems. How does the EHDS Regulation affect me?

When manufacturers of medical devices, in-vitro medical devices and/or high-risk AI systems *claim* these products are interoperable with EHR systems, they must prove compliance with the essential requirements for the interoperability component and the logging component for EHR systems. Please refer to Annex II for the requirements for these components[10]. Please note that the section 'general requirements' refers to requirements that apply to *both* harmonised components.

The Medical Device Regulation (MDR) and the In Vitro Device Regulation (IVDR) are currently undergoing a targeted revision[11]. As a consequence, the provisions of the MDR and IVDR referenced in the EHDS Regulation might have to be adapted following that revision.

Manufacturers of medical devices, in-vitro medical devices and high-risk AI systems are obliged to prove compliance with the essential requirements on the European interoperability software component for EHR systems and the European logging software component for EHR systems but are not under an obligation to use the European digital testing environment referred to in Article 40 of the EHDS Regulation. By contrast, the obligation to use the European digital testing environment to assess harmonised components is an obligation imposed to manufacturers of EHR Systems.

[10] There is an error in the cross-reference in the text: Article 27 refers to 'Section 2 of Annex II'; however, the text clearly refers to *both* harmonised components so, ultimately, all essential requirements listed in Annex II are relevant.

[11] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulations (EU) 2017/745 and (EU) 2017/746 as regards simplifying and reducing the burden of the rules on medical devices and in vitro diagnostic medical devices, and amending Regulation (EU) 2022/123 as regards the support of the European Medicines Agency for the expert panels on medical devices and Regulation (EU) 2024/1689 as regards the list of Union harmonisation legislation referred to in its Annex I.

Sources: Articles 27, 40 and Annex II

25. As a manufacturer of EHR systems, what steps do I have to take before I can place EHR systems on the market?

You will have to make sure that your EHR system complies with the requirements of the EHDS Regulation:

1) make sure that it provides the capabilities of the two harmonised components (see question 23 above);
2) prove that it does so by passing the tests in the European digital testing environment (see question 26 below);
3) draw up the technical documentation required under Article 37 of the EHDS Regulation and provide the information sheet required under Article 38 of the EHDS Regulation;
4) draw up the EU declaration of conformity in accordance with Article 39 of the EHDS Regulation;
5) affix the CE marking in accordance with Article 41 of the EHDS Regulation;
6) register your system in the Article 49 of the EHDS Regulation database.

Sources: Articles 30, 37 to 41, 49

26. As a manufacturer of EHR systems, what can I expect from the digital testing environment? When do I have to test my products?

The digital testing environments will test the two harmonised components of your EHR systems (see question 23 above) against the requirements in the EHDS Regulation.

You will have to do these tests before placing your systems on the EU market. You will receive a test report that will become part of your technical documentation referred to in Article 37 of the EHDS Regulation.

If your system does fails the tests, the report will provide feedback on which parts the system failed. You can then try again. The report that becomes part of the technical documentation referred to in Article 37 of the EHDS Regulation is the final, successful, one, showing that the two harmonised components of your EHR system passed all tests. Only the successful test report has to be made available[12].

[12] If your system fails the test, you are not permitted to place it on the market. The documentation obligations apply *when you place a system on the market.*

The Commission will develop the software for the European digital testing environment and make it available as open-source, so that Member States can deploy this environment where the two harmonised components of the EHR system components can be tested.

Sources: Articles 37(2), 40; recital 36

27. If a manufacturer updates a product, does it have to go through the conformity assessment process again?

Whether a product needs to go through the conformity assessment process again depends on whether the update amounts to a substantial change. This is the same concept of 'substantial change' as in other product legislation.

In short, an update counts as a substantial change when these three conditions are met:

(i) it modifies the original intended functions, type or performance of the product and this was not foreseen in the initial risk assessment;
(ii) the nature of the hazard has changed or the level of risk has increased because of the update; and
(iii) the product is made available / put into service.

Sources: Section 2.1 of the 'Blue guide' on product legislation

For buyers of EHR systems

28. As a hospital or other entity in the market for buying an EHR system, how do I find out if it complies with EHDS Regulation requirements?

There will be two ways:

1) EHR systems will have to be CE-marked (Article 41 of the EHDS Regulation). Look for the mark on the EHR system (if it has physical components) or in its documentation. The CE mark attests conformity with applicable requirements from in EU legislation.
2) Manufacturers will also have to register their EHR systems in a publicly accessible database managed by the Commission. The Commission will set up this database in due time before applicability of the registration requirement applies. You will be able to look up registered systems online.

Sources: Articles 41, 49; recitals 40, 51

29. Will healthcare providers, such as hospitals, have to update the EHR systems they have already deployed?

Healthcare providers will have to be able to export and import data in the European electronic health record exchange format (EEHRxF) (see question 16 above). That is a requirement they must comply with – how they achieve it is left to them. They could for example upgrade their existing EHR systems to support this feature or use a system that 'translates' between their internal file format and the EEHRxF. Member States can also require digital health authorities to provide additional instructions or national services to facilitate this.

Chapter III of the EHDS Regulation aims that all new EHR systems sold in the EU import and export data using the EEHRxF.

Sources: Articles 15(4), 23(5) and (6)

For users of wellness applications

30. What does it mean for a wellness application to claim interoperability with EHR systems?

This is a claim by the manufacturer of these apps or devices with connectivity features, that do not qualify as EHR Systems, due to the fact that they are used by individuals in a *context not related to healthcare provision or treatment* (see question 22). It means that the manufacturer of these app claims that it can provide information to EHR systems in a way that it can be used. An example would be a sleep tracker that can feed information to an EHR system.

When a manufacturer makes that claim, the wellness app must comply with common specifications and essential requirements for EHR systems.

Such interoperability does not mean that all information from the app will be continuously sent out. Apps can only export information when the user has consented to it and must offer control over what is sent and how – for example, the frequency ('send once a week') or triggering event ('send if indicator X exceeds value Y') (see Article 48(2)) of the EHDS Regulation for all the details).

Manufacturers that make these claims will have to register their wellness apps in the database established under Article 49 of the EHDS Regulation.

The labelling requirement provided in Article 47 of the EHDS Regulation is different from the requirements for placing EHR systems on the market and should not be confused with it.

Sources: Article 47; recitals 49 to 51

31. How do I find out whether a wellness application is interoperable with EHR systems?

Interoperable apps will have to be both labelled as such and registered in the public EU database set up under Article 49 of the EHDS Regulation. You will be able to look them up there.

Sources: Article 49; recital 51

Secondary Use (Chapter IV)

For data holders

32. Who is a data holder?

The definition of who qualifies as a health data holder in Article 2(2) point (t) of the EHDS Regulation includes several elements:

'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, developing or manufacturing wellness applications, performing research in relation to the healthcare or care sectors or acting as a mortality registry, as well as any Union institution, body, office or agency, that has either:

(i) the right or obligation, in accordance with applicable Union or national law and in its capacity as a controller or joint controller, to process personal electronic health data for the provision of healthcare or care or for the purposes of public health, reimbursement, research, innovation, policy making, official statistics or patient safety or for regulatory purposes; or

(ii) the ability to make available non-personal electronic health data through the control of the technical design of a product and related services, including by registering, providing, restricting access to or exchanging such data;

Any of the entities listed must make data under Article 51 available, provided they meet either of the two conditions in the indents.

However, Article 50 of the EHDS Regulation contains a carveout from the obligation to make data available for natural persons, such as independent researchers, and for micro-enterprises[13], unless the national law of the relevant Member State has provided for that the obligations of health data holders in the EHDS Regulation also apply to the natural persons and micro-enterprises. A healthcare provider that qualifies as a micro-enterprise would thus be excluded in principle from the obligation to make data available. However, if it grows so much that it no longer qualifies as a micro-enterprise, it would start to fall under the obligation.

Health data holders must make available data that falls under the Article 51 data categories (see question 0 below) and *that they control*. For example, if a manufacturer of a wellness application designs the

[13] See Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, http://data.europa.eu/eli/reco/2003/361/oj, OJ L 124, 20.5.2003, p. 36: micro-enterprises are those that employ fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million.

application in such a way that data is only kept locally on the app user's device without the manufacturer being able to access it, the manufacturer does not *hold* that data and thus would not be required to make it available.

To give another example, a provider of patient management systems processing personal electronic health data as a processor for a hospital does not qualify as health data holder for those data, as it does not meet the criterion of being a controller for the processing. In this situation, it would be the hospital as controller that would qualify as the health data holder.

Sources: Article 2(2) point (t); recitals 59, 63

33. What data will health data holders have to make available?

Where an entity qualifies as health data holder (see question 2), it will have to make the data categories listed in Article 51 of the EHDS Regulation available under the conditions in Chapter IV of the EHDS Regulation.
The data categories are listed in the table below. The obligation to make these categories available will apply in a staggered way. While most categories will have to be made available four years after the Regulation enters into force, i.e. as of 26 March 2029, the ones marked with an asterisk (*) will have to be made available six years after the Regulation enters into force, i.e. as of 26 March 2031.

Data category	Examples of what is covered	Examples of what is not covered
Electronic health data from electronic health records (EHRs)	EHRs contain a wide range of data about a patient's medical history, treatments, and outcomes generated by healthcare providers when providing treatment, such as diagnoses and lists of problems, medication lists and treatment plans.	An EHR kept by a healthcare provider that qualifies as a micro-enterprise (unless that Member State has also extended the duty to make data available to those entities, see Article 50(2)).
(*) Data on factors impacting on health, including socio-economic, environmental and behavioural determinants of health	For example, lifestyle factors analysis (smoking, alcohol consumption, surgeries, accidents...)	Detailed socioeconomic data collected outside healthcare settings, or purely environmental data not linked to health.
Aggregated data on healthcare needs, resources allocated to healthcare, the provision of and access to healthcare, healthcare expenditure and financing;	For example, resources allocated to healthcare covers data on the availability and distribution of healthcare resources, e.g. number of healthcare facilities (such as hospitals, clinics, nursing homes), number of healthcare professionals (e.g. doctors,	Individual-level information on healthcare expenditure.

	nurses, GPs), availability of medical equipment and technology. This is about aggregate-level non-personal data.	
Data on pathogens that impact human health;	Collections of information on pathogens that can cause disease in humans, including bacterial, viral, fungal, parasitic or prion pathogens:	data on pathogens only affecting animal health.
Healthcare-related administrative data, including dispensation, reimbursement claims and reimbursement data;	Collections of information that is generated through the administration of healthcare services, typically used for billing, reimbursement, and healthcare management purposes.	Banking data such as account numbers related to reimbursement.
(*) Human genetic, epigenomic and genomic data;	Human genetic data refers to the information contained in an individual's DNA, including their genes and chromosomes (e.g. genotyping data, genomic sequencing data, microarray data). Human epigenomic data refers to the information about the chemical modifications to an individual's DNA or histone proteins that can affect gene expression without altering the underlying DNA sequence (e.g. DNA methylation data, histone modification data) Human genomic data refers to the comprehensive information about an individual's genome, including their genetic and epigenetic data (e.g. whole-genome sequencing data, exome sequencing data, gene expression data).	
(*) Other human molecular data such as proteomic, transcriptomic, metabolomic, lipidomic and other -omic data;	Proteomic data from clinical research.	Raw molecular data generated for non-health related purposes.

Personal electronic health data automatically generated, through medical devices	Data from pacemakers or other implanted medical devices held by the manufacturer or healthcare provider	Data stored locally on devices and not accessible from the outside and aggregated data from medical devices.
Data from wellness applications;	Data from fitness trackers shared with health care providers or with the app developer.	Data stored locally on the user's device / in app to which the developer or healthcare provider does not have access
Data on professional qualifications, experience, practice and status, specialisation and institution of health professionals involved in the treatment of a natural person;	For example, whether a treating physician referred to in an EHR is a general practitioner or a specialist (and if so, in what field).	Contact information of that health professional.
Population-based health data registries (public health registries);	Population-based registries are systematic collections of health-related data from a defined population. These registries are typically maintained by government agencies, health organisations, or research institutions to support public health decision-making, policy development, and healthcare planning.	
Data from medical registries and mortality registries;	Medical registries are systematic collections of data on patients with a specific disease, condition, or characteristic, such as transplantation registries containing collections of data on organ transplantation outcomes, including patient characteristics, transplant procedures, complications, and graft survival rates.	

	Mortality Registries are a systematic collection of data on deaths, including information on cause, circumstances, and demographics, such as cause-of-death registries containing data on the underlying cause of death, including information on disease, injury, or condition.	
(*) Data from clinical trials, clinical studies and clinical investigations subject to Regulation (EU) No 536/2014, Regulation (EU) 2024/1938 of the European Parliament and of the Council, Regulation (EU) 2017/745 and Regulation (EU) 2017/746, respectively;	Data from completed clinical trials, investigations, and studies, subject to rules established in the legal acts governing them.	Data from ongoing trials, studies or investigations.
Other health data from medical devices	Aggregated data from medical devices held by manufacturer or healthcare provider	Data stored locally on a device to which the manufacturer or healthcare provider does not have or personal data falling under point (h)
Data from registries for medicinal products and medical devices;	Collections of data on the use, safety, and effectiveness of medicinal products and medical devices, including the two types of registries below: - Medicinal product registries: These registries collect data on medicinal products, including prescription and over-the-counter medications, vaccines, and biologics. - Medical device registries: These registries collect data on medical devices, including implantable devices, diagnostic equipment, and software.	

(*) Data from research cohorts, questionnaires and surveys related to health, after the first publication of the related results	Encompasses information collected from groups of individuals or populations to understand health-related phenomena, behaviours, or outcomes. These data are often used to identify risk factors, track trends, or evaluate the effectiveness of public health interventions. The requirement to declare these datasets only applies after the first publication of results.	
Health data from biobanks and associated databases	Electronic health data kept by repositories of biological samples and associated health data, which are collected and stored for research purposes. These repositories can contain a wide range of biological samples as well as associated health data, such as medical records, lifestyle information, and environmental exposures. Examples include: - Population-based biobanks: collections of data on biological samples and health data from large populations, often for the purpose of studying genetic and environmental factors that contribute to disease. - Disease-specific biobanks: collections of data on biological samples and health data from individuals with specific diseases. Tissue banks: collections of data on human tissue samples for research purposes.	The biological samples themselves held by biobanks. EHDS secondary use concerns the re-use of existing electronic health data, not about the generation of new data. EHDS secondary use cannot be used to request new analyses on biological samples (as that would then generate *new* data).

Please note that this covers the above data held by health data holders regardless of the date of data collection or registration– the obligation will also apply to all, existing electronic data.

Sources: Article 51, recital 55, 56

34. Is a health data holder of personal electronic health data always the controller? What about joint controllership situations?

As far as personal electronic health data is concerned, a health data holder is always *a* controller (see the reference to the 'controller' in the definition of 'health data holder' in Article 2(2) point (t) of the EHDS Regulation).

Where a processor processes personal electronic health data on behalf of a controller, it is the controller that is subject to the obligations as health data holder (provided the controller also meets the other criteria set out of in definition of 'health data holder').

In joint controllership situations, it is for the joint controllers to organise among themselves who will e.g. handle communication with the health data access bodies or provide dataset descriptions.

Sources: Article 2(2) point (t)

35. What kind of safeguards does the EHDS Regulation include for intellectual property and the protection of trade secrets?

Article 52 of the EHDS Regulation establishes a specific framework to protect intellectual property rights and trade secrets linked to health data made available under the EHDS.

It sets out the additional rules for making data available that could include these rights and trade secrets. The EHDS Regulation provides a framework that carefully balances the sharing of this health data with the need to protect intellectual property rights and trade secrets. The underlying principle is that under the EHDS, intellectual property rights and trade secrets should not be an obstacle to the re-use of data. However, the EHDS should not be used to circumvent the protection of these rights or of trade secrets, nor should it lead to a forfeiture of protection.

Health data holders will be able to notify to the health data access body (HDAB) if their datasets contain information covered by intellectual property rights or trade secrets. They can do this either when submitting the dataset description for inclusion in the dataset catalogue in accordance with Article 60(3) of the EHDS Regulation or later when a permit or request on such data is issued.

The HDAB is then responsible for ensuring that relevant protective measures are put in place. These measures may be of a legal, organisational or technical nature. They can, for example, include additional contractual arrangements between health data holders and data users as a condition for accessing the data. The Commission will draw up non-binding templates to cover these arrangements.

As an additional layer of protection, should the HDAB conclude that none of the protective measures that can be put into place are sufficient to safeguard the intellectual property rights or trade secrets, it can reject the permit application on those grounds.

The HDAB's decision can be challenged in court, both by the health data holder and by the health data user. The protective measures available to the health data holder under the applicable legal provisions regulating the intellectual property rights and trade secrets are not affected by the EHDS Regulation.

Sources: Article 52, recital 60

36. What are trusted health data holders and what is their role?

While the EHDS aims to make available data from a broad range of health data holders, it is also true that some health data holders have more experience and relevant skills than others. The concept of trusted health data holders in Article 72 of the EHDS Regulation acknowledges this.

Member States can designate trusted health data holders based on their ability to provide a secure processing environment, demonstrate the necessary expertise to assess health data access applications and health data requests, and provide the necessary guarantees to ensure compliance with the EHDS Regulation. Member States have the discretion to decide at national level whether to establish a procedure whereby health data holders are designated as *trusted* health data holders.

Following their designation, trusted health data holders may receive data permit applications forwarded by the health data access body (HDAB).

Sources: Article 72; recitals 76, 79

37. How will health data holders describe their datasets?

In accordance with Article 60(3) of the EHDS Regulation, health data holders will have to provide the relevant health data access body with descriptions of the datasets they hold. The detailed list of elements will be set out in an implementing act to be adopted by the Commission (see question 4).

Health data holders will have to review the descriptions they provided once a year at a minimum to ensure the descriptions are still correct.

Sources: Articles 60(3) and 77

38. What are health data intermediation entities and what is their role?

Health data intermediation entities are a tool to reduce the administrative burden on health data holders.

Member States can designate such health data intermediation entities to take over specific responsibilities of health data holders, particularly in terms of managing data access requests. This helps reduce the administrative burden on individual data holders by centralising the process through a single intermediary. For instance, a Member State might designate a public sector body managing a centralised electronic patient file as a health data intermediation entity. Member States can designate multiple health data intermediation entities. These entities would then interface with the health data access body (HDAB) on behalf of various hospitals and other healthcare providers (or other health data holders, as the case may be), ensuring streamlined data access while maintaining compliance with all regulatory requirements.

Data made available via a health data intermediation entity is still considered as originating from several health data holders. This means that it is not possible for such entities to be designated as trusted health data holders. Data made available via health data intermediation entities will always go through the normal application process at the HDAB.

Please note that while the data intermediation services referred to in Chapter III of the Data Governance Act have a similar name, their tasks are very different. The primary purpose of data intermediation services is to facilitate voluntary data sharing in a business-to-business context.

Sources: Article 50, recitals 59, 76

For data users

39. What is considered 'research' for EHDS purposes? Can only not-for-profit entities do 'research'?

The concept of 'research' in the EHDS Regulation is wide-ranging, as set out in recital 61: '*The notion of scientific research purposes should be interpreted in a broad manner, including technological development and demonstration, fundamental research, applied research and privately funded research. Activities related to scientific research include innovation activities such as training of AI algorithms that could be used in healthcare or care of natural persons, as well as the evaluation and further development of existing algorithms and products for such purposes*'.

The EHDS Regulation makes no distinction in terms of *who* can do research. Both not-for-profit and for-profit entities can carry out research. There is no requirement for entities that carry out 'research' under the EHDS Regulation to be public sector bodies. Entities such as SMEs, startups, and larger companies involved in development, innovation, and AI training can indeed be considered to be carrying 'scientific research' under the EHDS Regulation.

This is the same broad concept of 'research' as set out in recital 159 of the GDPR, and it includes research carried out by private-sector organisations (such as for the '*training of artificial intelligence algorithms that could be used in healthcare'*, which would often be done by private sector bodies). Activities that are considered as research under the GDPR should also be considered 'research' under the EHDS Regulation, as long as they also meet the specific requirements of Article 53(1)(e) of the EHDS Regulation.

Sources: Article 53(1) point (e), recital 61

40. Health Data Access Applications and Permits: future data extractions.

Data permits may foresee extractions of data, for data that will be made available in the future (e.g. request for annual updates to the dataset described in the health data application) only if the applicant and subsequently health data user is a public sector body or Union institution, body, office or agency. In this case the applicant needs to submit instead the information concerning the period for which the electronic health data can be accessed, the frequency of that access or the frequency of the data updates.

Unless this is the case, where the update frequency will be explicitly mentioned in the data permit, a new permit would be needed to access new data. This would also result in a new access instance in the Secure Processing Environment, adhering to the 'one permit per instance' rule.

Sources: Article 67(5), Article 68(12) and (13).

41. What is HealthData@EU?

HealthData@EU will be the cross-border infrastructure supporting secondary use under the EHDS Regulation. It will provide a federated, EU-wide dataset catalogue that prospective health data users can use to find datasets for secondary use from holders all over the EU. It will also provide a common application form that applicants can use to submit multi-country applications. The infrastructure will then forward the application to the relevant national contact points (who will then distribute it to the competent health data access bodies (HDABs) or to the relevant authorised participant. It will also provide tools for the cooperation between HDABs, for example so that they can share information on penalties imposed.

Moreover, if two or more national contact points or authorised participants request a secure processing environment, the Commission may also one that can be to make data available for analysis, operating in the same way as secure processing environments at national level.

Sources: Article 75, 63(7); recital 80

42. How will the data quality and utility label work?

The data quality and utility label will ensure greater transparency regarding the quality and utility of datasets made available for secondary use. This label will help health data users identify high-quality datasets by giving a general assessment as well as detailed evaluations across various characteristics, such as documentation and accuracy.

The label can both provide a general assessment of a dataset, with different levels, as well as a more detailed view by different characteristics (documentation, accuracy…). The details, including the different levels, will be set out by the Commission in a delegated act.

Labelling will be mandatory for datasets for which data collection was publicly funded (EU or national funding). This covers datasets for which the funding was specifically given for data collection purposes. For other datasets, providing a data quality and utility label is optional. For example, where public funding is used to set up a registry for research purposes, the label will be mandatory. Where a hospital receives public funding for providing treatment, the label will be optional, as the funding is for providing treatment, and recording data is incidental to that task.

Sources: Article 78; recital 85

For patients / data subjects

43. As an individual, can I opt out from secondary use?

Yes, you can. Article 71 of the EHDS Regulation grants you a right to opt out from secondary use.

Once you have opted out of secondary use under the EHDS Regulation, your personal electronic health data cannot be processed in response to any new data permits or requests approved after the date on which you exercised your right to opt out. The health data access bodies (HDABs) and health data holders must take the necessary steps to ensure that data related to individuals who have exercised their right to opt out is excluded from new processing activities. This does not affect the processing under permits or for generating replies to data requests approved *before* that date.

For example, if data, including that of natural person A is made available under a permit issued on day X and person A opts out on day X+10 days, the content of the secure processing environment referred to in Article 73 (SPE) will not change. The effect of an opt-out is for *future* data permits and requests issued, and does not retroactively apply to an individual's health data. Failing to do so would jeopardise the scientific integrity of the results – if data relating to person A were removed from the SPE in the example above, the health data user would get different results for the same statistical analysis on day X+9 and X+11. This would make it impossible to check that the analysis was correct.

Similarly, using the opt-out from secondary use under the EHDS Regulation does not affect other reporting obligations – for example, health professionals will still report notifiable diseases or suspected adverse reactions to medicinal products to the relevant authorities.

Sources: Article 71, recital 54

44. The right to opt-out of secondary use applies 'where personal electronic health data relating to [the data subject] can be identified in a dataset'. Does this mean that the right does not apply if a health data holder cannot identify a natural person in a dataset it holds (for example because it only holds pseudonymised data and cannot link it to the identifiers used to constitute the opt-out list)? What should health data holders and HDABs do in these situations?

Regarding disclosure by the health data holder to the health data access bodies (HDABs), this right would not apply in the above example. If a health data holder cannot identify a natural person in a dataset — such as when the data is pseudonymised and the holder cannot link it to identifiers used in an opt-out list— the right to opt-out of secondary use does not apply. This follows the same logic as in Article 11 GDPR which states that controllers should not process additional personal data only so that they can comply with data subject rights.

Please also note that the HDAB may carry out additional steps in preparing the data, which may also include screening the data against additional attributes that the opted-out person provided or other information available to the HDAB, but not to the health data holder. In that situation, the data relating to the person who has opted out would still be disclosed by the health data holder to the HDAB, but the HDAB would strip out the data when preparing the dataset for making it available in the secure processing environment (SPE). If also the HDAB is unable to identify the person, their data would be included in the SPE.

To give another example: if a health data holder holds data that might be identifiable (information in a registry 'patient with rare disease X, in age group Y, living in municipality Z'), it should not be obliged to proactively collect *additional personal data that it does not need for its own purposes*, in order to allow that patient to exercise their right to opt out, as that would create a tension with the data minimisation principle. On the contrary, the HDAB receiving the data from the health data holder is tasked with further processing that data, when preparing the datasets. Please also note that in any case, (attempting) reidentification is forbidden for health data users.

Sources: Articles 71, 61(3); recital 54

45. Are there exceptions to the right to opt-out of secondary use?

No, all natural persons (individuals) have the right to opt-out.

However, in specific exceptional situations the EHDS Regulation allows Member States to create mechanisms to also make data that relates to persons who have opted out available. See Article 71 of the EHDS Regulation, paragraphs 4 and following.

The text sets out rules for such mechanisms. Data relating to persons who have opted out can only be made available where in an individual case:

- the purpose of the data permit/request application is one of the purposes in Article 53(1) points (a) to (c) or where it is research under Article 53(1)(e), further qualified by a requirement that it be research for important reasons of public interest.
- the health data user is a public sector body or a Union institution, body, office or agency, including entities carrying out tasks for them (such as a contractor);
- the data cannot be obtained by alternative means in a timely and effective manner under equivalent conditions;
- the health data applicant has provided the relevant explanations why it wants to use this exceptional provision.

If a Member State has established this mechanism, prospective health data users can apply to use it as part of the data permit / data request application. It will be for the health data access bodies (HDABs) to decide whether to allow this, as part of the data permit / data request decision.

Sources: Article 71, recital 54

46. Is there a link between the rights to opt out of primary and secondary use?

No, they are independent of each other.

When a natural person has used an opt-out relating to primary use (where it exists - see question 13 above), that does not mean that the person also automatically opts out from secondary use. The same applies the other way around. It is possible for a natural person to use one opt-out, but not the other.

For health data access bodies (HDABs)

47. Is there a limit to how many HDABs a Member State can set up?

No, there is no limit. The text allows Member States to have multiple health data access bodies (HDABs), with no limit on how many HDABs they can designate. The tasks of HDABs can be assigned to multiple entities, for example based on the territorial and/or organisational scope.

For example, a Member State with multiple regional healthcare systems might decide to set up a different HDAB for each of them. A Member State may also decide to split tasks by function, for example splitting the tasks of permit/request approval and of providing secure processing environments into two separate entities. A Member State might also decide to have sectoral HDABs, splitting competencies based on the different data categories listed in Article 51.

Any entity assigned to carry out HDAB tasks and designated as an HDAB must comply with the requirements on HDABs (e.g. on reporting and funding).

If a Member State designates multiple HDABs, it must appoint one of them as a coordinator. The coordinator will for example be responsible for collating the activity report.

Sources: Articles 55, 57; recitals 64, 80

48. What happens if I want to contest the decision of an HDAB?

Article 81 of the EHDS Regulation gives both natural and legal persons the right to lodge a complaint related to the provisions of the on secondary use if they consider that their rights or interests are being negatively affected. Complaints can be lodged both individually and collectively with the relevant health data access body (HDAB). If for example a health data holder or a health data user wishes to contest the decision of an HDAB related to a permit that has been issued, this is the right instrument to do so.

However, when the complaint lodged concerns the rights of natural persons to opt out, such complaints should be transmitted to the relevant Data Protection Authority (DPA), responsible to supervise the GDPR. This ensures the smooth cooperation between health data access bodies (HDABs) and DPAs and guarantees a clear distinction between their remits.

An administrative decision issued by the HDAB, either in the form of a positive or negative response to a data permit application or a health data request, is not a prerequisite to lodge a complaint under Article 81. However, to bring an HDAB decision before a court, a party must challenge an existing administrative act to establish legal standing. A negative response to a health data application permit would constitute, for instance, such an administrative act. Therefore, if the applicant withdraws their request, the HDAB

cannot issue either a positive or negative reply regarding the withdrawn application. Consequently, there would be no administrative decision, leaving no grounds to challenge the matter in court.

Sources: Article 81, recital 99

49. Who carries out the pseudonymisation and anonymisation of data? The health data holder, the HDAB, or both?

Both health data holders and health data access bodies (HDABs) may be involved in the pseudonymisation and anonymisation of data under the EHDS Regulation, or, in some cases, just one of the two will be involved.

See recital 72: 'Taking into account the specific purposes of the processing, personal electronic health data should be pseudonymised or anonymised as early as possible in the process of making data available for secondary use. It should be possible for pseudonymisation and anonymisation to be carried out by health data access bodies or by health data holders.'

Here are two examples:

1) A data permit is issued for 'data items A-F relating to procedure G carried out in hospitals H to M in timeframe X-Z'. In this case, when extracting the data, the hospitals as health data holders could already strip out other data items (such as obvious patient identifiers) as a first pseudonymisation step. The HDAB would then be in contact with the hospitals for the details and may carry out further pseudonymisation steps.
2) A data permit is issued for 'data items A-F relating to medical procedures G and P carried out in hospitals H to M in timeframe X-Z, with data linkage in case patients underwent medical procedures G and P in different hospitals'. In this case, as procedures G and P may have been carried out in different hospitals (possibly without knowledge of each other), it may be necessary for the hospitals to include some patient identifiers (e.g. health insurance number or other identifier commonly used in the relevant healthcare system), so that the HDAB can make the link when preparing the data for provisioning in the secure processing environment referred to in Article 73 (SPE). However, those patient identifiers would not be made available to the health data user, only the information that 'lines X and Y refer to the same person' should be available. The HDAB will be in contact with the hospitals as health data holders for the details of these operations (such as hashing the identifiers before disclosure to the HDAB) and may carry out further pseudonymisation steps.

Ultimate responsibility for ensuring proper pseudonymisation and anonymisation rests on the HDAB. That said, the actual pseudonymisation or anonymisation might also be already carried out by the health data holder. Ensuring that data is pseudonymised or anonymised as early as possible in the process of making data available applies the principle of data minimisation in accordance with the GDPR.

Sources: Articles 57(1) point (b), 66(3); recital 72

For authorised participants

50. How can a data infrastructure, e.g. an ERIC or EDIC, become an authorised participant in HealthData@EU?

When applying for authorised participant status, such data infrastructures will have to undergo a compliance check to see if they meet the relevant requirements. The Commission will set out the detailed procedures as part of the implementing act under Article 75(12) point (b) of the EHDS Regulation).

Sources: Article 75(4); recital 80

51. What does becoming an authorised participant in HealthData@EU mean for a research infrastructure or other party?

Becoming an authorised participant means that, for example, entities can federate their data catalogues with the European dataset catalogue, which will make it easier to find their data. They will also be able to receive applications through the HealthData@EU infrastructure and may adopt decisions to grant or refuse access to the data within their remit (provided that their own legal framework grants them that power). In exchange, they will have to comply with certain rules under Chapter IV of the EHDS Regulation, for example they must provide their data catalogue in the same format as health data access bodies, to make it possible to federate data catalogues.

Sources: Articles 68; recital 80

Governance (Chapter VI)

52. What is the EHDS Board and what will it do?

The EHDS Board will be the main forum for the Member States and the Commission to cooperate and exchange information. The provisions establishing the EHDS Board will apply from 26 March 2027.

Member States will designate two representatives each, covering primary and secondary use aspects. A representative of the Commission will co-chair together with a representative elected from among the Member State representatives.

In the EHDS Board's main tasks are to assist Member States in coordinating their practices, to issue written contributions and exchange best practices on the implementation of the EHDS Regulation.

The EHDS Board can establish subgroups at working level to prepare these activities.

The EHDS Board can also cooperate with other relevant entities, such as ENISA and the EDPB. It can also invite external experts where appropriate.

The EHDS Board (and the steering groups, see question 53 below) will gradually take over the tasks of the current eHealth Network. During a transition period until 2031, they will co-exist, with the EHDS Board taking over as more and more parts of the EHDS Regulation will become applicable. As the eHealth Network focuses on primary use, this transition mainly affects primary use aspects.

Sources: Articles 92, 103; recital 95

53. What are the steering groups and what are their tasks?

The steering groups function at operational level. They are the fora in which practical decisions about the management and further development of the MyHealth@EU and HealthData@EU infrastructures will be taken.

Regarding MyHealth@EU, they will gradually take over the tasks of the current governance structure for infrastructure. During a transition period until 2031, they will co-exist, with the steering group for MyHealth@EU taking over as more and more parts of the EHDS Regulation will become applicable.

Sources: Article 95; recital 98

54. What is the stakeholder forum and what will it do?

The stakeholder forum complements the work of the EHDS Board by providing a venue for other stakeholders, such as healthcare providers, patient organisations, researchers, and industry. It will facilitate the exchange of information promote cooperation with those stakeholders. It will serve a similar purpose as the current eHealth stakeholder group.

Its members will be appointed by the Commission following a public call for expressions of interest.

Sources: Article 93; recital 97

International aspects (Chapter V)

55. Can non-EU countries participate in data exchanges for primary use?

Yes, but only under certain conditions.

National contact points of non-EU countries that want to join MyHealth@EU can undergo a compliance check where the Commission checks that legal, organisational, operational, semantic, technical and cybersecurity measures in the non-EU country are equivalent to those applicable to the Member States. When a non-EU country's national contact point passes this check, the Commission may adopt an implementing act to connect that national contact point to MyHealth@EU. Member States are involved in the adoption of these implementing acts.

When a non-EU country joins MyHealth@EU, its healthcare providers (via its national contact point) can exchange patient summaries and other priority categories the same way as the Member States among themselves. For example, when an EU citizen needs medical care in such a non-EU country, the health professionals treating the patient there will be able to retrieve the patient summary. It would also work the other way around, with health professionals in the EU receiving information from such a non-EU country.

The Commission will keep a public list of the national contact points of non-EU countries connected to MyHealth@EU. Each connected country, regardless of its status as a Member State or a non-EU country, will have one national contact point connected to the EU. Non-EU country national contact points will not be members of the MyHealth@EU steering group but they may be invited as observers – operational decisions about the management of the cross-border infrastructure will always be solely in the hands of the EU Member States only.

Contact points for relevant systems established at the international level can join MyHealth@EU the same way.

At the same time, it will still be possible to share data between Member States and non-authorised non-EU countries for the provision of healthcare outside the scope of the EHDS Regulation and the MyHealth@EU infrastructure. The EHDS rules apply within their own scope and do not affect any other existing bilateral cooperation and data exchanges. Such exchanges of personal data would still need to comply with the requirements set out in Chapter V of the GDPR.

Sources: Articles 24(3), 98(2), recital 35

56. Territorial scope: When will non-EU based entities be subject to health data holders' obligations? For example, what about a non-EU-based sponsor of a clinical trial that takes place in the EU?

The EHDS Regulation applies to health data holders established in the European Union. The term 'health data holder' is defined as any entity that operates within the health or care sectors, develops products or services for these sectors, or is an EU institution and meets the other requirements in Article 2(2) point (t) of the EHDS Regulation. The EHDS obligations do not apply to health data holders established in non-EU countries unless they have an established presence in the EU. For example, a non-EU-based sponsor of a clinical trial conducted in the EU would not be directly subject to the EHDS Regulation obligations unless it has an established presence in the EU. In such cases, the responsibility for complying with the EHDS obligations would fall on the EU-based establishment acting as controller or joint controller of the data. In the case of multinational companies, the entity controlling the means and purpose of processing the data will be considered the controller in accordance with the GDPR; consequently, it will be bound by the EHDS rules on data holders.

57. Will the EHDS Regulation apply in the EEA countries?

The EHDS Regulation is labelled as having EEA relevance. As for any act with this label, the EFTA Secretariat will launch a process to incorporate it into the EEA Agreement. For more information on the process, please see here. For the current state of the procedure, please see here.

Once the EHDS Regulation has been incorporated in the EEA Agreement, its rules will apply in the EEA countries as well.

Sources: EHDS title, EEA-Lex – factsheet 32025R0327

58. Can entities established in non-EU countries submit applications for data permits or data requests?

They can only do so in two situations:

1. Where they are established in a non-EU country that is recognised as giving data applicants established in the EU reciprocal access to health data held by holders established in that non-EU country; this reciprocal access must be recognised in an implementing act adopted by the Commission under Article 91(2) of the EHDS Regulation, or
2. where they are established in a non-EU country that has become an authorised participant in HealthData@EU under Article 75(5) of the EHDS Regulation. However, this possibility will only apply after a transitional period of ten years from the entry into force of the EHDS Regulation.

In both cases, this would only be possible after a Commission implementing act has been adopted. During the adoption process, known as comitology, Member States are actively involved and consulted prior to the vote and adoption of the act.

Sources: Articles 75, 91; recital 94

59. How does the EHDS Regulation interact with mechanisms for secondary use established in non-EU countries?

The EHDS Regulation's mechanisms for secondary use set out ways of cooperating with non-EU countries. Non-EU countries can become authorised participants in HealthData@EU (see Article 75(5) of the EHDS Regulation, which however applies only after a transitional period of ten years after the EHDS Regulation enters into force). This option allows them to for example federate dataset catalogues to make them searchable together with the European catalogue. Decisions about health data of holders established in the European Union will always be taken in the EU, never by non-EU countries.

Sources: Article 75(5)

Relationship with other EU law

60. How do the EHDS Regulation and the GDPR relate to each other?

The General Data Protection Regulation (GDPR) is the main text laying down EU data-protection law. It sets out rights for natural persons (individuals) whose personal data is processed and obligations for the controllers and processors who process that data. It also sets up a system of independent supervisory authorities to ensure that the rules are followed.

Regarding primary use, the EHDS Regulation complements the rights of natural persons established by the GDPR relating to their personal data with respect to specific categories of health-related data. For example, the EHDS Regulation complements natural persons' right to access their own data.

Under the GDPR, natural persons can request access to their personal data held by a controller. This is a broad-ranging right, allowing the person to ask for access to all (or parts of) the personal data that the controller holds on them. To respond to access requests, the controller will have to search for and collate the data from across their organisation. This takes time and effort. That's why, under the GDPR, controllers have up to a month to respond to access requests and can either refuse to act on or charge a fee for overly repetitive or manifestly unfounded requests.

However, in the health sector, people often need certain data right away and cannot afford to wait. That's why the EHDS Regulation establishes an additional targeted right for individuals to freely access certain categories of their own electronic health data, such as the patient summary. Access needs to be provided immediately, in practice using a kind of self-service portal. This then removes the need for the controller / healthcare provider to manually search for and collate the data. That's why there is no option for them to refuse frequent requests or charge for them.

The supervisory authorities in charge of the GDPR will also monitor the implementation of this new right under the EHDS Regulation.

Regarding controllers' and processors' obligations, the EHDS Regulation sets out specific tasks for entities processing personal data.

The GDPR sets out conditions for the lawful processing of personal data –simply put, 'what counts as a valid reason to process personal data?'. The processing of personal electronic health data under the EHDS fulfils these conditions. For example, the processing of personal data in the HDAB's secure processing environments will take place in line with the public interest task assigned to the HDABs by the EHDS Regulation (Article 6(1) point (e) GDPR). Health data holders will make data available to the HDABs based on a legal obligation established by the EHDS Regulation in conjunction with the individual data permit (Article 6(1) point (c) GDPR).

The GDPR also has specific requirements for lifting the general prohibition on processing special categories of personal data, such as health data. Often, this requires appropriate safeguards to be put in place (see

Article 9(2) point (j) GDPR, for example). The allowed purposes, the permitting process, the use of secure processing and other provisions in Chapter IV of the EHDS Regulation are just such safeguards which are laid down by law and which help ensure the processing operations are carried out safely.

Sources: Articles 1(3), 22; recitals 8, 9, 19, 20, 23, 34, 52

61. How do the EHDS Regulation and rules on medical devices relate to each other?

Where the manufacturer of a medical device or an in-vitro diagnostic medical device claims interoperability with the harmonised software components of EHR systems, it must prove compliance with the essential requirements for the two EHDS harmonised components. (see question 23 above).

If a product is both an EHR system *and* a medical device, it must meet the requirements of both regulations, including registration requirements (in the case of medical devices, it shall be registered in EUDAMED). As part of the implementation, the Commission will work to ensure that the two registrations can be done in a streamlined way. For registration requirements under the EHDS Regulation, see also question 28 above.

Sources: Articles 1(5), 27(1), 49(3); recitals 42, 51

62. How do the EHDS Regulation and the Clinical Trials Regulation relate to each other?

The EHDS Regulation works alongside the Clinical Trials Regulation (Regulation (EU) 536/2014)[14], which establishes the Clinical Trials Information System (CTIS), and related legal texts. The CTIS serves as a centralised IT platform for the submission, evaluation, and management of clinical trial applications as it is defined in the Clinical Trials Regulation. All relevant data on clinical trials applications are publicly available unless they are personal data or commercial confidential information.

As health data holders, sponsors and investigators of clinical trials and investigations can access a wide range of relevant data in order to complement or facilitate their work.

As indicated in the EHDS Regulation, this does not affect (regulatory) data protection rights enjoyed by holders of marketing authorisations. Data from clinical trials and investigations should only be made available under the EHDS after the trial or investigation has finished (see recital 56), although data may be shared earlier on a voluntary basis, and in line with the provisions of the Clinical Trials Regulation.

[14] Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC (Text with EEA relevance).

Sources: Article 1(3), recitals 56, 60

63. How do the EHDS Regulation and the Data Governance Act relate to each other?

The Data Governance Act (DGA), (Regulation (EU) 2022/868)[15] sets out rules for four main areas:

1) Chapter II: cross-cutting rules on *how* public sector bodies make data available;
2) Chapter III: rules on data intermediation services;
3) Chapter IV: rules on data altruism;
4) Chapter V: the possibility to categorise certain non-personal data as highly sensitive and impose specific safeguards for transfers of this data to non-EU countries.

These rules interact with the EHDS Regulation as follows:

1) The DGA sets out cross-cutting rules on *how* public-sector bodies make available data that is protected on the grounds of personal data protection, commercial confidentiality, including trade secrets, statistical confidentiality, and intellectual property rights. However, it does not create an obligation for public-sector bodies to make data available. If this obligation does exist, the DGA sets out the conditions that apply, for example regarding the fees that can be charged and the timelines for providing data. Put simply, the DGA says: '*if* a public-sector body (as a data holder) makes protected data available, here's *how* they need to do it'.
   The EHDS Regulation on the other hand says: 'health data holders *must* make these defined data categories available, and here's *how* they need to do it'.
   The addressees are also different: DGA Chapter II applies to public-sector bodies across all sectors (with some exceptions), while the EHDS applies to health data holders, which can be both public-sector bodies and private-sector entities.
   The scope of the data covered is different too: in principle, the DGA applies to all (electronic) data held by public-sector bodies (with some exceptions), while EHDS secondary use rules apply to the categories of electronic health data listed in Article 51 only, regardless of whether the holder is a public-sector body or a private entity.
   The main difference however is the actual obligations: the DGA does not require public-sector bodies, as data holders, to make data available. Meanwhile, the EHDS creates an obligation for health data holders to make available the categories of electronic health data listed in Article 51, subject to the conditions and criteria set out in the EHDS, especially the permitting process.
2) Data intermediation services under the DGA facilitate *voluntary* sharing of data between different data holders and/or data subjects. Making data available under the EHDS will be an *obligation* for health data holders. Intermediation services under the DGA and health data intermediation entities under the EHDS

[15] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance).

are separate concepts. Data intermediation services under the DGA can complement the structures provided for in the EHDS and support the collection, sharing or pooling of health data for certain other use cases.

3) Data altruism is a complementary framework for obtaining of e.g. personal health data for research, in particular from patients, based on consent. In this context, the EHDS Regulation sets out additional rules in one specific situation: when a data altruism organisation registered under the DGA makes health-related personal data available in a secure processing environment, that environment must meet the same requirements as secure processing environments under the EHDS.
4) The DGA includes an empowerment for delegated acts to provide for safeguards regarding transfers of highly sensitive non-personal data held by public sector bodies to non-EU countries. Non-personal data made available for secondary use under the EHDS qualifies as such highly sensitive data under certain circumstances (see Article 88(1)). In such cases, protective measures must be detailed in a delegated act under the DGA.

Please note that the Digital Governance Act is being repealed under the Commission proposal on the Digital Omnibus.[16] As a consequence, the provisions of the Digital Governance Act referenced in the EHDS Regulation might have to be adapted following that revision.

Sources: Articles 1(3), 62(2), 68(4), 73(4), 88; recitals 70, 78, 92

64. How do the EHDS Regulation and the Data Act relate to each other?

The Data Act, (Regulation (EU) 2023/2854)[17] sets out rules for the following topics:

1) business to consumer and business to business data sharing;
2) contractual data sharing;
3) emergency access to data by public sector bodies and certain EUIBs;
4) requirements concerning data processing services.

They interact with the EHDS Regulation as follows:

1) Internet-of-Things (Chapter II of the Data Act): The rules on data sharing in Chapter II of the Data Act require that connected products and related services to be designed in such a way that 'product data and

[16] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus) COM/2025/837 final.

[17] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (Text with EEA relevance).

related service data, including the relevant metadata necessary to interpret and use those data, are, by default, easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format, and, where relevant and technically feasible, directly accessible to the user' and set out rules for the sharing of such data. They apply in the relation between the manufacturer/provider of such products/services and their customer who may be a consumer or a professional. In short, users have the right to receive such data and to share it with third parties of their choosing, under certain conditions. Where an EHR system or a medical device, including related apps, qualifies as a connected product / related service, those requirements will apply to it. It's important to note that these requirements are about data sharing with the user or on the initiative of the user – for example sharing telemetry data of a device with a third party for additional analytics.

A 'user' in the sense of the Data Act is a person that has contractual rights *in rem* on the connected product. The clearest situation is ownership, i.e. when a patient at their own cost acquires a diagnostic tool. A 'user' is also a person that rents or leases a medical device at their own expense. In other situations, diagnostic equipment may only be put at disposal as part of the diagnostic process (e.g. long-term ECG measurement) without the patient acquiring a right *in rem* in relation to the diagnostic equipment in accordance with national civil law or social security legislation. Patients may in certain situations request the porting of health data from connected diagnostic or therapeutic equipment which they own or rent at their own expense in a primary use (Chapter II of the EHDS Regulation) situation but there is no possibility for compensation between healthcare providers sending and receiving data (Article 18 of the EHDS Regulation). Patients may also wish to make available health data from connected diagnostic or therapeutic equipment which they own or rent at their own expense voluntarily for the purpose of research and innovation ('data altruism', see previous question) and are then not bound by the data categories and usage categories foreseen in Chapter IV of the EHDS Regulation.

2) Further rules on business-to-business data sharing and dispute settlement (Chapter III of the Data Act): The rules on obligations for data holders obliged to make data available pursuant to Union and national law in the Data Act apply to data sharing in a business-to-business context. Making data available for secondary use under the EHDS Regulation is not business-to-business data sharing under the Data Act. However, for the settlement of disputes on the level of fees, Article 62(4) of the EHDS Regulation establishes that health data holders and users shall have access to dispute settlement bodies in accordance with Article 10 of the Data Act.
3) Emergency Access to Data (Chapter V of the Data Act): The rules on emergency access to data by public sector bodies and certain EUIBs in Chapter V of the Data Act are formulated as a 'last resort' possibility. Secondary use under the EHDS Regulation is *not* emergency access under the Data Act. Emergency access under the Data Act can only be used where there is no other feasible channel to have the data be made available. The rules on secondary use in the EHDS provide for exactly such a channel. Where secondary use under the EHDS Regulation can provide a feasible channel to make data available, emergency access under the Data Act is *not* an option. However, in cases where Data Act emergency access is used, health data access bodies under the EHDS may provide support (Article 51(2) of the EHDS Regulation).
4) Data Processing Services (Chapter VI of the Data Act): The requirements on data processing services in Chapter VI of the Data Act relate to providers of such services, such as cloud hosting providers, and impose requirements on them to make it easier for their clients to switch away from them. Where a secure processing environment (SPE) provider provides its services in a way that they also qualify as a data

processing services under the Data Act, the obligations established there *also* apply to it in its relationship with its customer (e.g. an HDAB that has contracted out the provision of an SPE).
To give an example: in the Data Act, data processing services are defined as (among other elements) providing access to a 'shared pool of configurable, scalable and elastic computing resources'. If an SPE provider provides an SPE in such a way, then it is in scope of Chapter VI of the Data Act for its relation to the HDAB as its customer. If an SPE provider provides an SPE using a dedicated server for a customer (as opposed to a shared pool), that service is outside the scope for Chapter VI of the Data Act.

Please note that the Data Act is undergoing revision under the Commission proposal on the Digital Omnibus.[18] As a consequence, the provisions of the Data Act referenced in the EHDS Regulation might have to be adapted following that revision.

Sources: Articles 1(3), 18, 51(2), 57(4); recitals 61, 70

65. How do the EHDS Regulation and the Artificial Intelligence Act relate to each other?

The EHDS Regulation and the Artificial Intelligence Act (AI Act, Regulation (EU) 2024/1689)[19] intersect in cases where an Electronic Health Record (EHR) system incorporates AI functionalities. A product may fall under both the AI Act and the EHDS Regulation: imagine an EHR system that not only documents treatment, but also includes an AI system that provides emergency triage functions (see Annex II, point 5(d) of the AI Act). This system would then be subject both to the requirements for high-risk AI systems under the AI Act, and for EHR systems under the EHDS Regulation. In such cases, the conformity assessment procedures should be organised in a way that limits the administrative burden on manufacturers (see recital 42 EHDS Regulation).
One way in which the EHDS itself already limits this burden is through the rules on registering EHR systems: if an EHR system is *also* a high-risk AI system and thus needs to be registered in the EU database for high-risk AI systems (see Article 71 of the AI Act), the two registrations can be done in a streamlined way.

Sources: Articles 1(5), 27(2), 49(3); recital 42

[18] *Idem.*
[19] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance).

66. How do the EHDS Regulation and the Cyber Resilience Act (CRA) relate to each other?

Both the Cyber Resilience Act (CRA, Regulation (EU) 2024/2847)[20] and the EHDS Regulation provide for rules for making EHR systems available on the market. The CRA lays down essential cybersecurity requirements *for products with digital elements*, while the EHDS Regulation provides, amongst other things, essential requirements, including interoperability and logging requirements, and further obligations to be complied with for EHR systems.

A product may be a product with a digital element as defined in the CRA and an EHR system as defined in the EHDS Regulation at the same time. Article 32(5a) of the CRA, which was introduced by the EHDS Regulation determines that in such cases the conformity assessment procedure of the EHDS Regulation should apply instead of the procedure of the CRA.

Example: A computer that has been designed for storing and viewing patient summaries while delivering healthcare services, could be a product with digital elements under the CRA that is also an EHR system, under the EHDS Regulation.

Both the CRA and the EHDS Regulation provide for conformity assessment procedures respectively applicable to each category of products they cover. In the case of the CRA this assessment applies to products with digital elements, whereas under the EHDS Regulation this applies to the harmonised software components of EHR systems (as defined in Article 25(1) of the EHDS Regulation).

However, this does not mean that manufacturers need to ensure the assessment of conformity of the cybersecurity of a product through the procedures set out in both the CRA and the EHDS Regulation in cases where such product is covered by both regulations.

For more information on how to comply with both the CRA and the EHDS Regulation requirements please consult the FAQs document on the CRA implementation.

Sources: Articles 104, 25(1), Cyber Resilience Act Article 32(5a)

67. What is the interplay between the EHDS Regulation and the EU framework for coordinating social security systems?

The EHDS Regulation complements many of the cross-border healthcare rights provided by the EU framework for coordinating social security systems, as it facilitates the exchange of personal electronic

[20] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance) PE/100/2023/REV/1 *OJ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj*.

health data that may be necessary for a natural person to receive healthcare in another Member State. For instance, the cross-border sharing of patient summaries, a priority category of personal electronic health data, under EHDS can enable this for individuals moving between EU Member States.
At the same time, the EHDS Regulation does not set out any rules on social security, nor does it replace the actual proof of insurance status given by the European Health Insurance Card or the Portable documents S1 or S2. The EHDS Regulation fully respects the right of the Member States to determine social security benefits and organise their national healthcare systems. The EHDS Regulation does not interfere with existing obligations requiring national competent institutions to provide insured persons with information on their rights under the EU framework for coordinating social security systems.

Sources: Article 14(1) point (a)