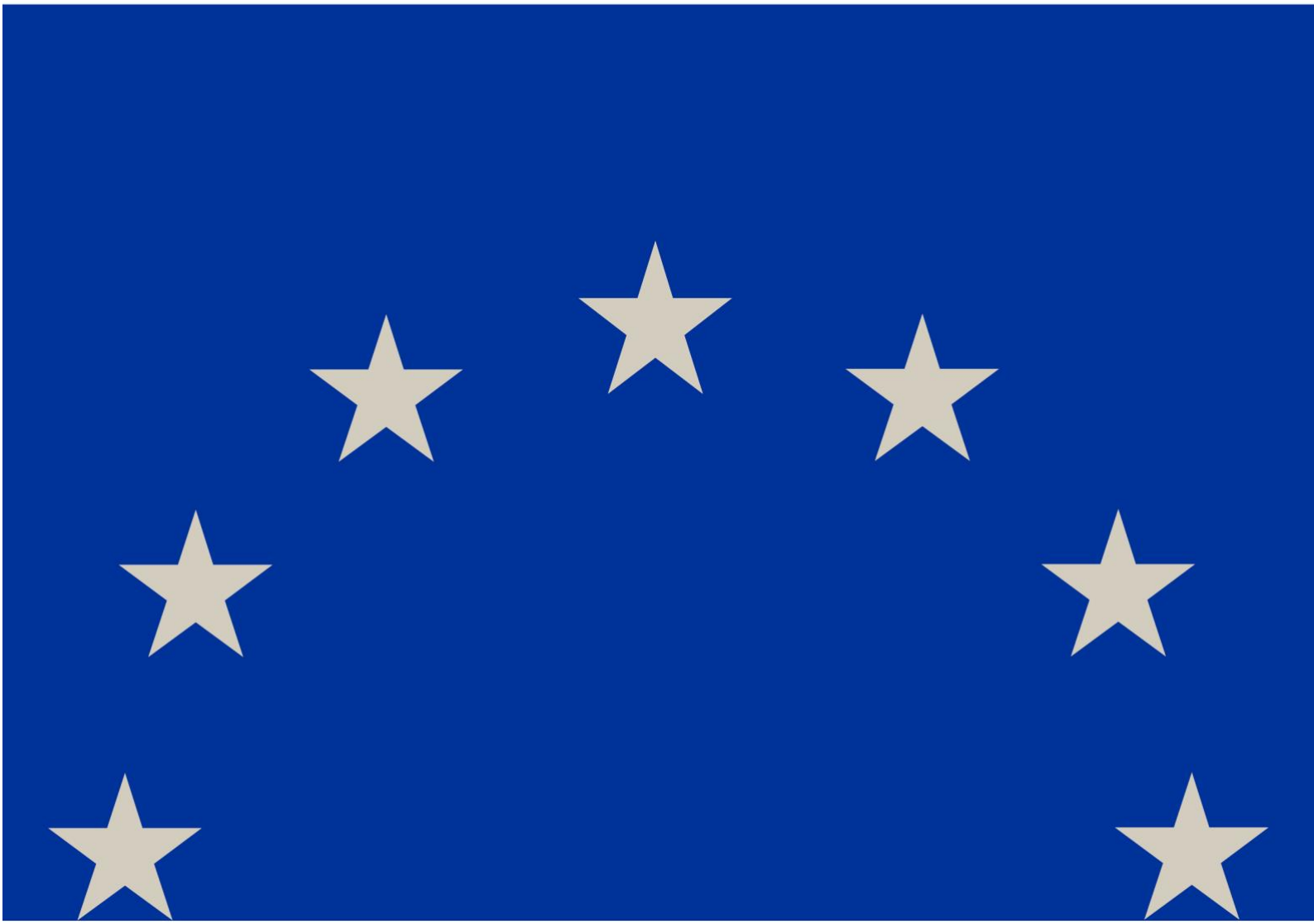
European Commission

DG SANTE
Unit C.1 – Digital Health

Frequently Asked Questions on the European Health Data Space

Last updated 5 March 2025



Frequently Asked Questions on the European Health Data Space

Last updated 5 March 2025

Contents

Introduction

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

This document should not be considered as representative of the European Commission's official position. The replies to the frequently asked question do not extend 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.

This is a living document that may be updated in the future. It complements other communications products related to the European Health Data Space. 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 5 March 2025.

Version	Date
1.0	05/03/2025

General

1. What is the aim of the EHDS?

The EHDS Regulation has three main parts, each with different addressees:

Chapter II on primary use provides additional rights to patients and establishes the technical infrastructure necessary for their implementation. 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 creates 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 is addressed to health data holders and users. It creates obligations on health data holders to make data available and frames how health data users can use such data. It establishes health data access bodies (HDABs) as well as the necessary infrastructure.

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

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

On the definition of the material scope, see Article 1, paragraphs 3 and following, notably:

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

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

(9)(b) – this clarifies that the EHDS 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 laid down by law to obtain that data and cannot use the EHDS for this purpose.

Sources: Article 1, Recital 63

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

The EHDS Regulation was published in the Official Journal on 5 March 2025 and enters into force 20 days after. However, it will start to apply in a phased way:

- Key provisions of Chapters II (on primary use) and III (on EHR systems) will apply from 4 years from entry into force, i.e. by 26 March 2029, regarding the first group of priority categories (patient summaries, electronic prescriptions, electronic dispensations) and from 6 years, i.e. by 26 March 2031, for the remaining priority categories (medical imaging studies, test results, discharge reports).
- Chapter IV on secondary use will apply from 4 years from entry into force regarding most of the data categories listed in Article 51, so by 26 March 2029. For some categories, such as genetic data, it will apply from 6 years after entry into force, so by 26 March 2031 (see also question 28). Article 75(5) on the possibility for third countries to become authorised participants in HealthData@EU will apply from 10 years after entry into force, that is to say by 26 March 2034.

In practical terms:

As a patient, you will be able to use the health data access services and exercise your rights in primary use from entry into force by 26 March 2029 for the first group of priority categories (patient summary, 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 for 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 HDAB by 26 March 2029 or 2031, depending on which of the Article 51 categories (see Q0 below) each dataset falls into. By the same time, 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 applications to HDABs for permits and requests relating to most of the data categories in Article 51 by 26 March 2029. From 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 for example have to set up their digital health authorities and designate their national contact points by 26 March 2027. By 26 March 2029, they need to ensure that the services under Chapter II are up and running. By 26 March 2031, they will have to extend these to the second group of priority categories.

Regarding secondary use, by 26 March 2031, their HDABs must be ready to receive applications, as well as be connected to HealthData@EU. By two years later, the HDABs must be ready to also exercise their tasks regarding the final categories of data.

Other provisions, such as those on Governance and the setup of the EHDS Board will apply from entry into force plus two years, 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 on how the EHDS will operate. But there are plenty of technical details that will be set out in delegated and implementing acts – from the technical specifications of the European electronic health record exchange format to the 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 are set out, the systems will need to be built, tested, and deployed.

That is why the EHDS Regulation includes a deadline for the Commission to adopt key implementing acts by 26 March 2027: 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 by entry into force plus four years.

The key implementing acts with this deadline are the following:

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

Sources: Article 105; Recital 115

5. What is the Commission doing to support Member States as well as healthcare providers and other stakeholders for the application of the EHDS?

The Commission funds multiple projects and joint actions in preparation for the implementation of the EHDS. Please see some examples below:

Xt-EHR – working on implementation guides, technical specifications, and a conformity assessment framework for the adoption of the 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. About which kinds of data can I exercise my EHDS rights as a patient?

Under the EHDS Regulation, you will have an additional right 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, 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 problems, medication, vaccination, plan of care, 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 have these additional rights on the first three categories by 26 March 2029 (first phase) and by 26 March 2031 for the last three categories (second phase).

These rights apply to these data categories when such data are processed electronically. For example, a discharge report that exists only on paper would be out of scope.

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.

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 (see Article 4). These online services will provide you with a dashboard to for example access (view) your own data, see who accessed it, signal inaccuracies, restrict data, and manage your proxy authorisations (on proxy services, see also question 15).

Of course, access to these services will be secured. Authentication for accessing these services will use secure electronic identification methods, recognised under Article 6 of the eIDAS Regulation 910/2014. Often, national eIDs will qualify as such (see also question 19 below).

There is an additional design requirement for these services to be easy to use, for example for persons with disabilities, vulnerable groups, or people with low digital literacy.

Sources: Articles 4, 16; Recital 20

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

The EHDS will grant you the right to immediate access to the priority categories of your electronic health data through an 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. You will be able to download the data as well.

There are however two restrictions to this right of access:

First, the text acknowledges that there may be cases where due to the need for technological practicability, there can be slight delays in data availability. For example, there may be a short time lag between for example the time that a laboratory report is issued and when it shows up in your dashboard in the health data access service.

Secondly, there can be cases where immediate access to certain information could be harmful. 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.

Think for example 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 in 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, in accordance with Article 5, 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 29).

The EHDS Regulation does not establish a list of data elements that can be inserted. However, the intention is to enable patients to complement data in the priority data categories.

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

This right is only about *adding* information, it does not allow *changing (or deleting)* information provided by health professionals (for correcting errors in such 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 identify 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 it if needed.

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

Sources: Article 6, Recital 13

11. How will the EHDS enhance portability of data for me as a patient?

Article 7 will significantly enhance 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 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 Art. 7 EHDS 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 Art. 7 EHDS 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 ports data to support the same format. The EHDS creates an obligation on both side 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 transport the data yourself. Instead, your data can be transmitted from its source to the treating health professional. 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 work for patients? What is the effect on health professionals?

The right to restrict allows patients to limit the visibility of certain parts of their electronic health data in the priority categories that can be shared. Other data that have not been restricted will remain available via the services set up under the EHDS.

Data that have 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 the EHDS Regulation.

However, there will be an exception: in critical situations, health professional may invoke a 'breaking the glass' mechanism – for example when an unconscious patient arrives in an emergency room, the treating health professionals 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?

The EHDS allows Member States the option to provide patients with the right to opt out from 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 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, for instance, be unable to access their own 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 through the EHDS health professional access service, such as retrieving a patient summary. For example, a new treating health professional would not be able to use the health professional access service to obtain the patient summary of such a person. However, Member States may also establish exceptions similar to the 'breaking the glass' scenario that can apply to this right.

Also note that this full opt-out from primary use in EHDS 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 the other way around (see question 0 below).

Sources: Article 10, Recital 18

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

The right to restrict means that patients will be able to limit the visibility of specific parts of their electronic health data in the priority categories, so that only selected data are accessible. Patients can also restrict health professionals' access to <u>all</u> their data in the services set up by the EHDS. However, there will be a

possibility for a 'breaking the glass' scenario allowing access to restricted data in emergencies. Other data that have not been restricted will remain available via the services set up under the EHDS. This is a right granted directly by the EHDS Regulation.

Such restrictions do not impact other rights of natural persons under the EHDS. For instance, the patients themselves can still exercise the right of access to their health data, 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, persons will have the right to withdraw their electronic health data completely from the data exchanges *set up by the EHDS*. If a patient exercises this right, all their data will be excluded from the EHDS data exchanges for primary use, meaning for example that health professionals or the patient themselves cannot access their patient summary or other data through the access service provided by the EHDS. Please note that this 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. An example would be a person authorising their spouse to access that person's records.
2. A legal guardian acts on behalf of their wards. The main example here are parents for their minor children. In this case, the relevant Member State's rules on such guardianship apply – the legal guardian's access could for example be nuanced depending on whether the child is a toddler or a teenager.

Sources: Article 4; Recitals 20, 21

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

One of the main obstacles to ensuring 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 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 interoperability of electronic health information. 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 through an implementing act, to be adopted within two years of entry into force of the EHDS Regulation, that is to say by 26 March 2027 (see Article 15 EHDS).

The specifications are expected to build on the work of the XT-EHR Joint Action that 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.

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 cross-border. The Commission will provide central services as a service to the Member States. The Member States' national contact points will connect to this infrastructure. The actual exchanges of electronic health data will be point-to-point: as an example, if you need medical care abroad in Member State B, the healthcare provider there can receive your patient summary from Member State B's national contact point, who will have requested it via MyHealth@EU from Member State A, where you usually live.

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 an evolution of the currently existing infrastructure of the same name that already supports exchanges of patient summaries, electronic prescriptions and electronic dispensations between several Member States, currently on a voluntary basis. The difference is that connecting to MyHealth@EU under the EHDS will become mandatory for Member States and that the scope of data to be exchanged will increase.

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 will provide you with access to the priority categories of data relating to the patients under your treatment. This will improve the information available to you 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.

The Member State where you work will set out detailed rules on this access – for example on distinguishing access rights among 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 distinguishes access rights between nurses and medical 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 have the right 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 (see Article 16 EHDS Regulation). 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. Their use could continue as long as they are compliant with commons specifications to be adopted through implementing acts under the EHDS Regulation (Article 36). At the same time, health professional access services provided by public sector bodies or by private parties (except small and medium size enterprises) will always have to accept the European Digital Identity Wallets where the requirements of Article 5f(1)-(2) of Regulation 910/2014 are met.

Additional steps beyond basic electronic identification of the user are needed to verify the health professional's professional qualifications. The reason 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 plain words, they prove that 'this person is indeed Jane Doe' – but 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 the EU Digital Identity Wallets, will also enable provision of proof of qualification or sharing other attributes, and the use of this functionality could be considered by Member States.

Sources: Articles 12 and 16; Recital 29

For Member States' authorities

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

The Digital Health Authorities will have the tasks listed in Article 19 of the EHDS Regulation. They will be responsible for orchestrating 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 the implementation of the new rights for patients, providing relevant information to patients, health professionals and healthcare providers.

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.

Member States are entitled to organise their healthcare systems as they see fit, so this is an obligation of results – what matters is that the services are operational and accessible. The way they are provided, e.g. whether they are directly provided by the state or by other actors entrusted with such tasks in the national systems is thus left open for Member States. The access services should be linked to the 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?

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 of software or just software: an EHR system can be integrated as part of a physical device or be software on its own;
- They allow the storage, intermediation, export, import, conversion, editing, or viewing of priority categories of electronic health data (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 to be considered as an EHR system;
- They are intended by their manufacturer to be used:
    - By healthcare providers when providing patient care: the classic example would be 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: this means that for example an app that connects to the electronic health data access service for patient will count as an EHR system.

This definition is wide, and it is so on purpose: to ensure interoperability throughout the chain of connected systems. It does not only apply to systems that aggregate information, like hospital information systems, but also to the systems 'feeding' them.

Article 25(2) and recital 38 clarify that when general purpose software is used for these 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 providing patient care[1] and so does not count as an EHR system.

[1] 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.

Products may have parts that fall under different certification systems such as under the Medical Devices Regulation[2], the Artificial Intelligence Act[3] or the EHDS. In such case, each part of the product needs to comply with the applicable certification framework.

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 access electronically health data documents produced in the provision of healthcare services that are included in the priority categories under 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.
- A system converting the output of legacy EHR systems into the EEHRxF.

Out of scope:

- Scheduling system for appointments in a general practitioner's practice;
- Administrative billing system, unless it processes diagnosis, medication or other patient data from priority categories for preparing the bills;
- A wellness application processing non-medical data, e.g. sleep information or measuring intensity and duration of physical activity.

Sources: Articles 2(2), point (k), 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 Union, EHR systems must contain the two harmonised software[4] components, namely:

- The interoperability component,
- and the logging component.

These 'components' describe capabilities of EHR systems.

[2] 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, p. 1–175.

[3] 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.

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

The interoperability component provides the capability to import/export data that falls under the priority categories (see question 6) in the EEHRxF. There is no requirement that EHR systems 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.

Manufacturers will be obliged to test these components in automated testing environments (see question 25 below) prior to 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 define specific rules for the procurement or financing of, or reimbursement for EHR systems. The EHDS requirements 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. 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 automated testing environment (see question 25 below);
3) Draw up the technical documentation required under Article 37 and provide the information sheet required under Article 38;
4) Draw up the EU declaration of conformity in accordance with Article 39;
5) Affix the CE marking in accordance with Article 41;
6) Register your system in the Article 49 database.

Sources: Articles 30, 37 to 41, 49

25. As a manufacturer of EHR systems, what can I expect from the Automated Testing Environment? When do I have to test my products?

The automated 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 market in the Union. You will receive a test report that will become part of your system documentation.

If your system does not pass, the report will provide feedback on which parts the system did not pass. You can try again.

The report that becomes part of the system documentation is the final, successful, one, showing that the system passed all tests. Only the successful test report has to be made available[5].

The Commission will develop the software for the automated testing environment, so that Member States can deploy an automated testing environment where these components can be tested.

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

26. 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 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

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

There will be two ways:

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

Sources: Articles 41, 49; Recitals 40, 51

[5] If your system does not pass, you must not make place it on the market. The documentation obligations apply *when you place a system on the market.*

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

The requirement for healthcare providers will be to be able to export and import data in the 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 mandate digital health authorities to provide additional instructions or national services to facilitate this.

The rules in Chapter III of the EHDS Regulation will ensure that all new EHR systems offered in the Union will can import and export data using the EEHRxF.

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

For users of wellness applications

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

This is a claim by the manufacturer of such apps or devices (that are not themselves EHR systems). It means that the manufacturer of such 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. They can only export information when the user has consented to it and must offer control over what is sent and how – examples could be with which frequency ('send once a week') or triggering event ('send if indicator X exceeds value Y') (see Article 48(2)).

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

This labelling requirement is something different than the requirements for placing EHR systems on the market and should not be confused with it.

Sources: Article 47; Recitals 49 to 51

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

Any such app will have to be both labelled as such and registered in the public EU database established under Article 49 of the EHDS. You will be able to look them up there.

Sources: Article 49; Recital 51

Secondary Use (Chapter IV)

For data holders

31. 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 available, provided they meet either of the two conditions in the indents.

However, Article 50 contains a carveout from the obligation to make data available for individual natural persons, such as independent researchers, and for micro-enterprises[6]. For example, a healthcare provider that qualifies as a micro-enterprise would be excluded from the obligation to make data available. Should it however grow so much that it would no longer qualify as a micro-enterprise, it would start to fall under the obligation.

These entities 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 application in such a way that data is only kept locally on the app user's device without a possibility for that manufacturer to access it, the manufacturer does not *hold* that data and thus would not be required to make such data 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 health data holder.

[6] 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.

Sources: Article 2(2)(y); Recitals 59, 63

Which data will health data holders have to make available?

Where an entity qualifies as health data holder (see question 31), it will have to make the data categories listed in Article 51 available under the conditions in Chapter IV of the EHDS.

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 from entry into force plus four years, the ones marked with an asterisk (*) will have to be made available from entry into force plus six years.

Data category	**Examples for what is in scope**	**Examples for what is out of scope**
electronic health data from 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 diagnosis and problem list, medication lists and treatment plans.	EHR kept by a healthcare provider that qualifies as a micro-enterprise (unless that Member State extended the duty to make available data also to such 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, nurses, GPs), availability of medical equipment and technology. This is about aggregate-level non-personal data.	Individual-level information on healthcare expenditure
pathogen 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:	Pathogen data on pathogens only affecting animal health
healthcare-related administrative data, including dispensation, 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	Collection of health-related data that is generated by medical devices and kept by a health data holder.	Data stored locally on devices and not accessible from the outside.
data from wellness applications;	Data from fitness tracker shared with health care providers or with the app developer.	Data stored locally on user device / in app without access by the developer or healthcare provider
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	Data from pacemakers or other implanted medical devices held by manufacturer or healthcare provider	Data stored locally on device without access by manufacturer or healthcare provider
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 two types of registries: 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	Encompasses information collected from groups of individuals or populations to understand health-related phenomena, behaviours, or outcomes. These data are often used to identify	

related to health, after the first publication of the related results	risk factors, track trends, or evaluate the effectiveness of public health interventions. The requirement to declare such datasets applies after the first publication of result only.	
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: 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 is about 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 (that would then generate *new* data).

Note that this covers such data held by health data holders independently of the data's collection or registration date – the obligation will include old, existing electronic data.

Sources: Article 51, Recital 55, 56

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

Yes, as far as personal electronic health data is concerned, a health data holder is always *a* controller (see the inclusion of the "controller" element in the definition of "health data holder" in Article 2(2)(t)).

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

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

Sources: Article 2(2) point (y)

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

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

It sets out the additional rules for making data that could include such rights and trade secrets available. The EHDS provides a framework that carefully balances the sharing of such 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 such rights and of trade secrets either and should not 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 data catalogue 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 access to the data. The Commission will develop templates for such 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 refuse 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.

Sources: Article 52, Recital 60

34. 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 acknowledges this.

Trusted health data holders are entities that have been designated by Member States based on their ability to provide a secure processing environment, demonstrate expertise in data management, and meet specific guarantees related to the handling of health data. Following designation, trusted health data holders may receive data permit applications forwarded by the Health Data Access Body (HDAB). The trusted health data holder is then responsible for assessing these applications and providing recommendations to the HDAB. However, the HDAB still retains the final authority to approve or refuse the applications. If a permit is granted, the trusted health data holder may also take on additional tasks, such as preparing the data for secure access by the health data user.

Sources: Article 72; Recitals 76, 79

35. How will health data holders describe their datasets?

Health data holders will have to provide descriptions of the datasets they hold to the relevant HDAB. The detailed list of elements will be determined via an implementing act to be adopted by the Commission.

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

Sources: Articles 60(3) and 77

36. 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 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. Such 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 data intermediation services under Chapter III of the Data Governance Act have a similar name, their tasks are very different. Those services primarily serve to facilitate voluntary data sharing in a business-to-business context.

Sources: Article 50, Recitals 59, 76

For data users

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

The notion of 'research' in the EHDS is wide, see 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 does not distinguish by *who* does 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 be public sector bodies. Entities such as SMEs, startups, and larger companies engaged in development, innovation, and AI training can indeed be within the scope of "scientific research" under the EHDS.

This is the same wide notion of 'research' as 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 be considered the same under the EHDS.

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

38. What is HealthData@EU?

HealthData@EU will be the cross-border infrastructure supporting secondary user under the EHDS. It will provide a federated, Union-wide dataset catalogue that prospective health data users can use to find datasets for secondary use from holders all over the Union. 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 HDABs) or to the relevant authorised participant. It will also provide tools for the cooperation among HDABS, for example to share information on penalties imposed.

As part of HealthData@EU, the Commission will also provide a secure processing environment that can be used – upon request of two or more national contact points or authorised participants – to make data available for analysis, in the same way as secure processing environments on the national level.

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

39. How will the Data Quality and Utility Label work?

The data quality and utility label will provide 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 offering 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 for the collection. 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 the registration of data is incidental to this task.

Sources: Article 78; Recital 85

For patients / data subjects

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

Yes, you do. The EHDS Regulation grants you a right to opt out from secondary use under it.

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 opt-out date. The Health Data Access Bodies (HDABs) and health data holders must take necessary steps to ensure that data related to opted-out individuals 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 those of natural person A are made available pursuant to a permit issued on day X and person A opts out on day X+10 days, the content of the SPE will not change. The effect of an opt-out is for *future* data permits and requests. The reason for this is that otherwise, the scientific integrity of results would be jeopardised – if the 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 checking the correctness of analyses impossible.

Similarly, using the op-out from secondary use under the EHDS 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

41. The right to opt-out in secondary use applies "where personal electronic health data relating to [the data subject] can be identified in a dataset". Does this mean that 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), the right does not apply? What should health data holders and HDABs do in such situations?

Regarding the disclosure by the health data holder to the HDAB, this right would not apply then. If a health data holder cannot identify a natural person in a dataset —such as when the data is pseudonymised and the holder lacks the ability to link it to identifiers used in an opt-out list— the right to opt-out in 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 cannot 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*, as that would create a tension with the data minimisation principle. Please also note that in any case, (attempting) reidentification is forbidden for health data users.

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

42. Are there exceptions from the right to opt-out in secondary use?

No, the opt-out is a right for all natural persons.

However, in specific exceptional situations the EHDS Regulation allows Member States to create mechanisms to also make data relating to persons who have opted out available. See Article 71, 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 permit/request application is one of the purposes in Article 53(1)(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 an EUIB, including entities exercising tasks for them (such as a contractor);
- the data cannot be obtained by alternative means in a timely and effective manner;

- the health data applicant has provided the relevant explanations why it wants to use this exception.

If a Member States has established such a mechanism, prospective health data users can apply for it as part of the data permit / data request application. It will be for the HDAB to decide whether to allow this, as part of the data permit / data request decision.

Sources: Article 71, Recital 54

43. Is there a link between the opt-outs in primary and secondary use?

No, they are independent of each other.

When a natural person has used an opt-out in 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

44. 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 HDABs, with no limit on how many HDABs they can designate. The tasks of HDABs can be assigned to multiple entities, for example by territorial and/or organisational scope.

For example, a Member State with multiple regional healthcare systems might decide to set an 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 task and of providing secure processing environments into two separate entities. A Member State might also decide to have sectoral HDABs, splitting competencies by the different data categories listed in Article 51.

Any entity assigned 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

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

Both or either health data holders and Health Data Access Bodies (HDABs) may be involved in the pseudonymisation and anonymisation of data under the EHDS Regulation.

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.’

To give 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, the hospitals as health data holders could already strip out other data items (such as obvious patient identifiers) when doing the data extraction 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 received 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 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.

Final 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 follows the principle of data minimisation.

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

For authorised participants

46. 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 go through 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)(b)).

Sources: Article 75(4); Recital 80

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

Becoming an authorised participant means that entities can for example federate their data catalogues with the European dataset catalogue, which will increase the findability of 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 EHDS Chapter IV, for

example they must provide their data catalogue in the same format as health data access bodies, to allow federating data catalogues.

Sources: Articles 68; Recital 80

Governance (Chapter VI)

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

The EHDS Board will be the main forum for the Member State and the Commission to facilitate cooperation and exchange information. The provisions establishing the 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 Member State representative elected among them.

Its 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.

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

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

The Board (and the steering groups, see question 49 below) will gradually take over the tasks of the current eHealth Network. During a transition phase until 2031, they will co-exist, with the EHDS Board taking over as more and more parts of the EHDS will become applicable. As the eHealth Network focuses on primary use, this transition mainly affects primary use aspects.

Sources: Articles 91, 93, 103; Recital 95

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

The steering groups operate at an 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 phase until 2031, they will co-exist, with the steering group for MyHealth@EU taking over as more and more parts of the EHDS will become applicable.

Sources: Article 94; Recital 98

50. 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 exchange of information promote cooperation with them. It will serve a similar function as the current eHealth stakeholder group.

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

Sources: Article 92; Recital 97

International aspects (Chapter V)

51. Can third countries participate in the exchanges for primary use?

Yes, but only under certain conditions.

National contact points of third 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 such a third country are equivalent to those applicable to the Member States. When a third 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 such implementing acts.

When a third 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 third country, the treating health professionals 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 third country.

The Commission will keep a public list of third countries' national contact points connected to MyHealth@EU. Third 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 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.

Sources: Articles 24(3), 94, Recital 35

52. 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 within 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)(u). The EHDS obligations do not apply to health data holders established in third countries unless they have an establishment within 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 obligations unless it has an established presence within 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.

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

The EHDS Regulation is labelled as having EEA relevance. Like for any act labelled as such, the EFTA Secretariat will launch the process to incorporate it into the EEA Agreement. For more information on the process, please see here.

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

Sources: EHDS title

54. Can entities established in third countries submit applications for data permits or data requests?

They can only do so in two situations:

1. Where they are established in a third country that is recognised as providing reciprocal access to data applicants established within the European Union to health data held by holders established in that third countries via an implementing act adopted by the Commission pursuant to Article 90(2) of the EHDS Regulation, or
2. where they are established in a third country that has become an authorised participant in HealthData@EU pursuant to Article 75(5) of the EHDS Regulation. However, this possibility will only apply after a transitional period of 10 years from the entry into force of the EHDS Regulation.

Sources: Articles 75, 90; Recital 94

55. How does the EHDS interact with mechanisms for secondary use established in third countries?

The EHDS' mechanisms for secondary use provide for ways of cooperating with third countries. There is a possibility for third countries to become authorised participants in HealthData@EU (see Article 75(5) of the EHDS Regulation, which however applies only after a transitional period of 10 years from the entry into force of the EHDS Regulation). This allows them to for example federate dataset catalogues to make them searchable together with the European catalogue. Decisions about health data of holders established within the European Union will always be taken in the EU, never by third countries.

Sources: Article 75(5)

Relation with other Union law

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

The GDPR is the main text of Union data protection law. It sets out rights for natural persons whose personal data are processed and obligations on the controllers and processors who process them. It also sets up a system of independent supervisory authorities to ensure that those rules are followed.

Regarding primary use, the EHDS complements the rights of natural persons provided by the GDPR relating to their personal data in specific categories of data relating to health. The EHDS complements for example natural persons' right of access to their own data.

Under the GDPR, they can ask for access to their personal data a controller holds about them. This is a broad right, allowing the person to ask for access to all (or parts of) the personal data that controller holds about them. To reply to access requests, the controller will have to search for and collate the data across their organisation. This takes time and effort. That's why under the GDPR, controllers have up to a month to reply 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 now and cannot afford to wait. That's why the EHDS establishes an additional targeted right of 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 possibility 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.

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

The GDPR sets out conditions for the lawful processing of personal data – in simple words, 'what counts as a valid reason to process personal data?'. The processing of personal electronic health data under the EHDS fits into these conditions. For example, the processing of personal data in the HDAB's secure processing environments will happen based on the task in the public interest assigned to the HDABs by the EHDS Regulation (Article 6(1)(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)(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 the implementation of appropriate safeguards (see e.g. Article 9(2)(j) GDPR). The allowed purposes, the permitting process, the use of secure processing and other provisions in Chapter IV of the EHDS Regulation are such safeguards laid down by law and contributing to the safety of the processing operations.

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

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

Where the manufacturer of a medical device or 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 implementation, the Commission will work to ensure that the two registrations can be done in a streamlined way. For registration requirements under the EHDS, see also question 27 above.

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

58. How do the EHDS and the CTR relate to each other?

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

Sponsors and investigators of clinical trials and investigations as health data users can benefit from a broad access to relevant data in order to complement or facilitate their work.

As indicated in the EHDS Regulation, it does not affect (regulatory) data protection 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), without prejudice to earlier voluntary data sharing, and in line with the provisions of the Clinical Trials Regulation.

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

59. How do the EHDS and the DGA relate to each other?

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

1) Chapter II: Horizontal 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: A possibility to deem certain non-personal data highly sensitive and impose specific safeguards for transfers of such data to third countries.

These rules interact with the EHDS as follows:

1) The DGA sets out horizontal rules on *how* public sector bodies make available data that are protected on grounds of protection of personal data, commercial confidentiality including trade secrets, statistical confidentiality, and intellectual property rights. It does not however create an obligation for public sector bodies to make data available. If there is such an obligation, the DGA

sets out conditions, for example on the fees that can be charged and the timelines for providing data. In simple words, 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 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 scope of addressees is 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 or private sector entities.
The scope of the data covered is different: the DGA in principle 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, but independently of whether the holder is a public-sector body or a private entity.
The main difference however are the actual obligations: the DGA does not lay down an obligation on public sector bodies as data holders to make data available. The EHDS creates an obligation for health data holders to make the categories of electronic health data listed in Article 51 available, subject to the conditions and criteria set out in the EHDS, notably 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* on health data holder. Intermediation services under the DGA and health data intermediation entities under the EHDS 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 to enable the obtaining of e.g. personal health data for research, in particular from patients, based on consent. In this context, the EHDS Regulation adds rules in one specific situation: when a data altruism organisation registered under the DGA makes personal data related to health 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 of transfers of highly sensitive non-personal data held by public sector bodies to third countries. Non-personal data made available for secondary use under the EHDS qualify as such highly sensitive data under certain circumstances (see Article 87(1)). For such cases, protective measures shall be detailed in a delegated act under the DGA.

Sources: Articles 1(3), 62(2), 68(4), 73(4), 87; Recitals 70, 78, 92

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

The Data Act (DA, Regulation (EU) 2023/2854) 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 on data processing services.

They interact with the EHDS as follows:

1) Internet-of-Things (Chapter II of the Data Act): The rules on data sharing in Chapter II of the Data Act create a requirement that connected products and related services be designed in a way that 'product data and 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 data on the initiative of the user – for example sharing telemetry data of a device with a third party for additional analytics. **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 EHDS) situation** but there is no possibility for compensation between healthcare providers sending and receiving data (Article 18 EHDS). 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 EHDS.
2) 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 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 establishes that health data holders and users shall have access to dispute settlement bodies in accordance with Article 10 of the Data Act. 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 is *not* emergency access under the Data Act.** Emergency access under the Data Act can only be used where there is no other feasible other 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 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)).
3) 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 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 a 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 a SPE provider provides an SPE in such a way, then it is in scope of Chapter VI Data Act for its relation to the HDAB as its customer. If a SPE provider provides an SPE using a dedicated server for a customer (as opposed to a shared pool), that service is out scope for Chapter VI Data Act.

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

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

The European Health Data Space (EHDS) Regulation and the Artificial Intelligence Act (AI Act, Regulation (EU) 2024/1689) 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: 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) AI Act). Such a system would then be subject both to requirements for high-risk AI systems under the AI Act, and for EHR systems under the EHDS. In such cases, the conformity assessment procedures should be organised in a way that limits administrative burden on manufacturers (see recital 42 EHDS).

One way in which the EHDS itself already limits such burden are 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 AI Act), the two registrations can be done in a streamlined way.

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