White Paper

European Health Data Space (EHDS): A Comprehensive Guide to Data Reuse

A comprehensive guide to prepare for the reuse of health data under the EHDS regulation

PHILIP HINES, IQVIA
OLIVIA LOUNSBURY, Oxford University
ELENA SOFIA MASSACESI, Oxford University
JENNY GONG, Oxford University
LARISSA CHAN, Oxford University
HANNE VAN BALLEGOOIJEN, IQVIA
GEORGE GARRARD, IQVIA
CHRIS VAN BRONCKHORST, IQVIA

Table of contents

Executive summary

The European Health Data Space (EHDS) is an initiative by the European Union aimed at creating a unified framework for the secure and ethical reuse of electronic health data across the EU for research, innovation, and policy. The EHDS will benefit patients by providing easier access to their health records across borders and greater control over their data. Healthcare providers and patients will experience improved continuity of care, while researchers and the pharmaceutical industry will gain access to large-scale, high-quality health data. Policymakers and regulators will have a robust foundation for monitoring public health.

The EHDS distinguishes between EHDS1 for the primary use of health data (e.g., patient care) and EHDS2 for the secondary use of health data (e.g., research, innovation, policy making), with this document specifically focusing on the latter.

The operation of EHDS2 involves three key stakeholders: Health Data Holders (HDHs), which are organisations that control electronic health data; Health Data Access Bodies (HDABs), which are public sector bodies managing data access for secondary use; and Health Data Users (HDUs), which are individuals or organisations granted access to electronic health data for secondary purposes. In addition to discussing the requirements for each stakeholder, this document highlights potential challenges and solutions they may face in implementing the EHDS2. Specifically:

- **Health data holders** should establish an internal cross-functional EHDS group to prepare their compliance. This could include people dealing with IT, legal, data entry, depending on the organisation. This team should help prepare to catalogue electronic health data assets and to evaluate their capacity and capability for data provision and other EHDS2 obligations
- **Health data access bodies** will require significant investment and staffing to operate. The main challenges include successfully establishing a National Catalogue of health data, evaluating health data applications, processing the health data, setting up a 'Secure Processing Environment' (SPE) where the data can be accessed and analysed, and monitoring compliance and security. To succeed in their role, they need to ensure trust and compliance through stakeholder engagement from the outset
- **Health data applicants and users** will need to carefully prepare their applications. This could include building sample analysis models and requesting pre-submission consultations with HDABs. To respect the 18-month deadline for publishing results, HDUs may need to plan their research accordingly and utilise the extension exceptions, if needed

The combined challenge for all EHDS2 stakeholders is to establish a health data network, which is useable and sustainable. There are examples of successful, and less successful, health data networks, although the scale of EHDS2 is significantly larger, lessons should be learned from these past experiences. We have taken these lessons to identify the challenges, provide you with directions on how to overcome these challenges and successfully implement your requirements.

Should you want to discuss implementing the EHDS, email info@iqvia.com, we would love to hear from you.

Document aims

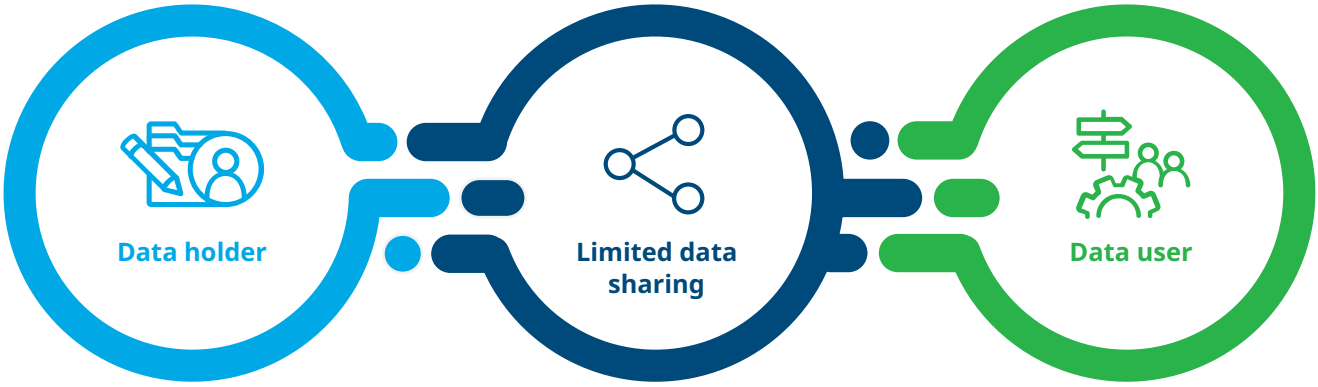
This document offers a comprehensive guide to reusing health data under the EHDS, with practical recommendations for HDHs, HDUs and government bodies such as HDABs.

Background

Health data access today

Electronic health data access across the EU is currently hindered by fragmented regulations (including GDPR implementation), varying software and hardware (infrastructure), and limited ability to exchange and use information (technical and organisational interoperability). This fragmentation affects patients, healthcare professionals, researchers, and policymakers alike, making it difficult to use health data effectively for individual care, public health, research, and innovation (See Figure 1).

Figure 1: Limitations of data sharing in the current health data landscape



Patients	**Due to**	Patients
Healthcare providers	Private data assets	Healthcare providers
Government orgs	Paper-based data	Government orgs
Research orgs	Cost of access	Research orgs
Industry	Legal barriers inc. GDPR	Industry
	Difficulty of anonymisation	
	Limited data interoperability	

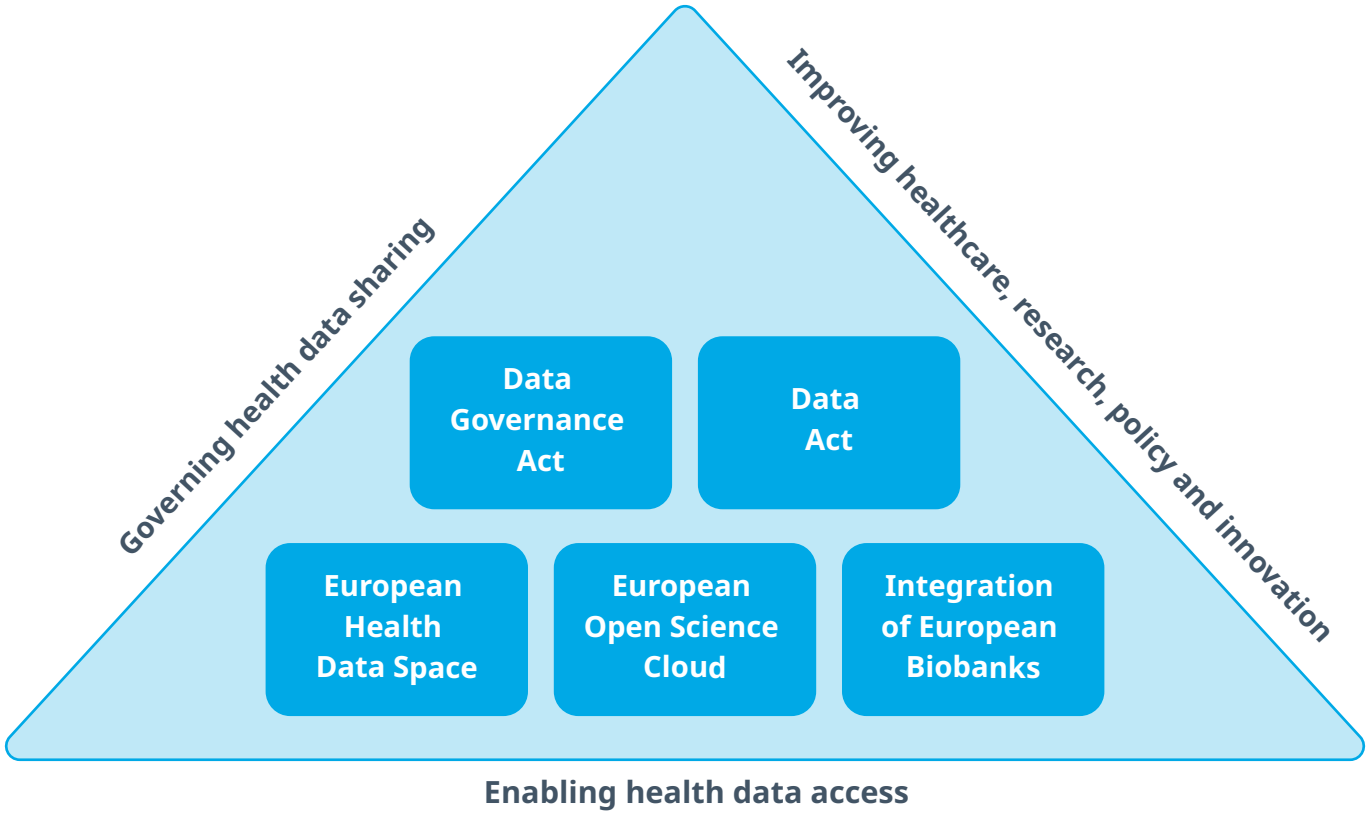
Source: The European health data revolution

EHDS — The enabler

The European Health Data Space (EHDS) is a direct response to these challenges. The EU Regulation enables the secure and ethical access and reuse of health data across the EU for healthcare, research, innovation, and policymaking.

It builds on existing data regulations and frameworks, in particular the GDPR and the European Data Governance Act, but introduces new actors, workflows, and infrastructure (See Figure 2). The concept of an EHDS has been envisaged for over 10 years but has now the legal basis to implement it. See Appendix 1 for more information on its governance structure within the EU.

Figure 2: Structure of the European Health Data Space



Source: The European health data revolution

EHDS1 versus EHDS2

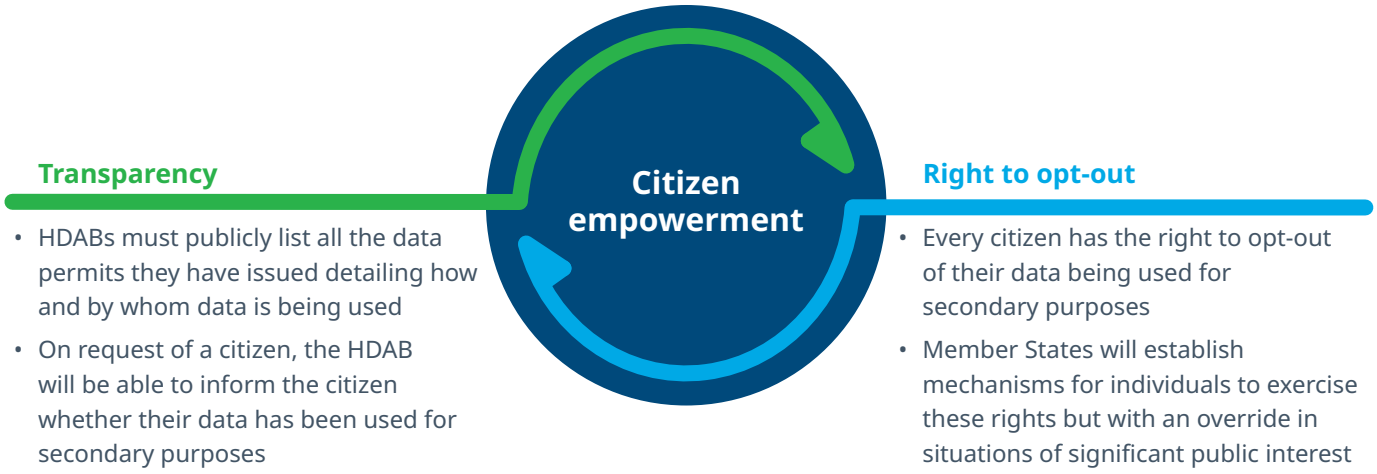
The EHDS distinguishes between EHDS1 for the primary use of health data (e.g., using a patient's health data to deliver their healthcare) and EHDS2 for the secondary use of health data (e.g., the re-use of health data beyond an individual's care for research, innovation, policy, or regulation). Citizens can opt-out of having their data available for sharing within EHDS. See Figure 3. See Appendix 2 for more information about the difference between primary and secondary use. **This document will focus on the secondary use of health data (EHDS2).**

EHDS2 — ENABLING DATA REUSE

The EHDS2 is set to benefit patients, healthcare providers, researchers and the life sciences industry, alongside policymakers and regulators.

For patients, it promises secondary use of health data, advancing the understanding of their disease and treatment, and enabling improved treatments regimes. The EHDS2 will be an opt-out system in which personal data will be anonymised and cannot be used for purposes like advertising. For healthcare providers, it offers the potential for data-driven improved care. For researchers and the pharmaceutical industry, the EHDS unlocks opportunities to access high-quality real-world data on a large scale, which could accelerate the development of new medicines and treatments. For policymakers and regulators, it provides a robust foundation for monitoring public health and evaluating the effectiveness of healthcare.

Figure 3: Citizen empowerment within EHDS2



One important clarification is that the EHDS doesn't affect existing data sharing routes or agreements, rather it offers a new route for health data sharing in the EU.

The EHDS will need to consider lessons learnt from previous analogous initiatives (Table 1).

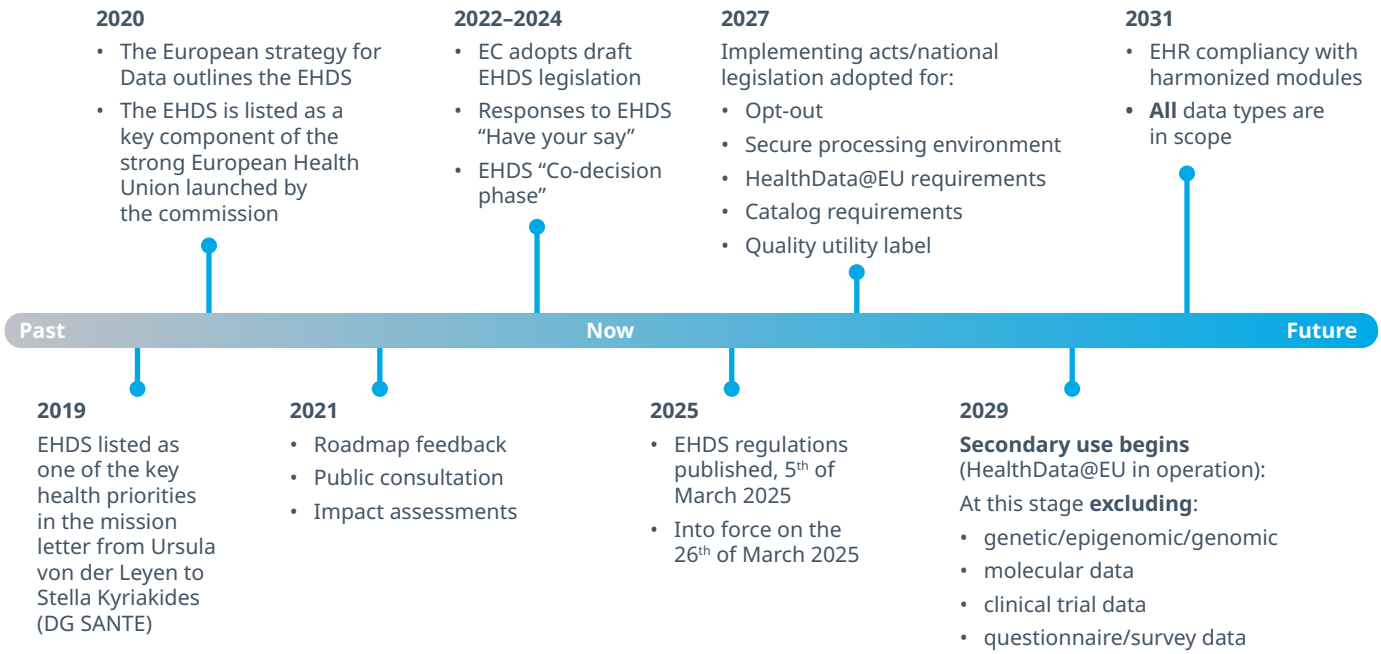
Table 1. Key lessons for EHDS implementation from other data networks

NETWORK INITIATIVE	COUNTRIES/ REGION	TYPE OF DATA	LESSONS LEARNED
CORE (IQVIA)	Global, including EU countries	EHR Claims, Lab, Registry	• Strong data governance and compliance in data sharing are essential for cross border data use • AI-driven analytics are powerful but depend heavily on fit-for-purpose data quality
EHDEN (IMI/ Erasmus MC)	22–29 EU countries	EHR, Claims, Lab, Medication	• Data silos remain a major barrier • Implementation requires alignment across policies and policymakers and in terms of data quality
DigiONE (IQVIA)	Europe (13+ countries via 6 centres)	EHR, Molecular Diagnostics	• Limited and unstructured digitalization requires Natural Language Processing/Optical Character Recognitions for free-text extraction • Reducing complexity by focussing on relevant data points only with MEDOC as reference model and evolve from there on
SAIL Databank (Welsh TRE)	UK (Wales)	EHR, Social care, Administrative	• Governance and information assurance must be established from the outset • Data linkage and quality are critical success factors
SNDS (France)	France	Claims, Hospital, Mortality, Social care	• Governance, access procedures and data usability remain bottlenecks • Linkage of the administrative claims dataset with additional data types increases its utility
PCORnet (USA)	United States	EHR, Claims, Patient-Reported Outcomes	• A Common Data Model (CDM) is essential for interoperability and scalability • Governance and data quality require continuous alignment among partners

EHDS2 implementation timeline

The EHDS regulation was published on 5 March 2025 and entered into force on 26 March 2025, marking the beginning of the transition phase toward application. The implementation timeline extends until 2031 with key milestones each year. Major milestones for EHDS2 will begin from 2029, but preparedness is starting now. See Figure 10.

Figure 4: EHDS2 implementation timeline



How EHDS2 will work — The process

The process for accessing and using health data under the framework is designed to be systematic, secure, and transparent. It is coordinated by Health Data Access Bodies (HDABs) and involves a series of structured steps, as depicted in Figure 5 for health data applications, Figure 7 for health data requests and the key deadlines listed in Table 2.

Figure 5: Steps involved in the reuse of electronic health data under EHDS

Step 1: Discovering data via National Catalogues (HDH, HDAB, HDU)

Each HDAB must establish and maintain a national health data catalogue (See Figure 6).

This catalogue lists all health datasets and metadata about them, including the data source, scope, quality, structure, and format of the datasets, enabling HDUs to identify data relevant to their research or policy questions.

HDHs are legally required to register their datasets in these national health data catalogues and keep the information up to date.

Figure 6: Data quality and utility label — Explained

HDH may also apply a 'data quality and utility label' with a deeper data description. This is mandatory for data generated with public funding and will include:

- **Data documentation:** Metadata, supporting docs, data dictionary, format/standards, source, (if applicable) data model
- **Technical quality:** Completeness, uniqueness, accuracy, validity, timeliness, consistency
- **Data quality management:** Maturity of processes (review, audit), bias examination
- **Coverage:** Period, population, (if applicable) representativity, average time for individual appearance
- **Access and provision:** Time from collection to dataset, time to provide data after approval

Step 2: Submitting a data access application (Applicant/HDU)

Once a relevant dataset is identified, the HDU formally requests the data from the HDAB in one of two ways:

1. **Health data access application:** Involves seeking access to the electronic health data. Once the Permit has been granted, this data can only be accessed within the SPE. Where it contains data pertaining to an individual, it must be provided in an anonymised or pseudonymised format. Additionally, the HDU must publish the results of the health data access application. Therefore, this request type is suited for conducting detailed research or for Artificial Intelligence model development, for example
2. **Health data request:** Requests can be submitted for the purposes referred to in EHDS Article 53. The HDU receives only anonymised, statistical results from the HDAB. The Health Data Request also requires a less detailed application and is faster than a Health Data Access Application. Therefore, this type of data request may be better suited for descriptive and exploratory research or feasibility studies, for example

If the request or application is approved by HDAB, the HDAB will instruct HDHs to provide the requested data. For data applications, the HDAB has up to three months to provide a permit, the HDH has three months to prepare the data, and the HDAB has up to two months to make the data available within the SPE. However, these timelines vary based on the type of request. See TEHDAS2 for more information about the different request types and their requirements.

The application must specify purpose, requested data, duration, legal basis, methodology, data protection measures, and confirm compliance with prohibited-use and reporting. The applications must also demonstrate that the requested data is proportionate and limited to what is strictly necessary to answer the research question. The HDH will also be expected to provide an estimate of its fees at this stage. The data may not be used for any purpose not explicitly outlined in the approved application.

Step 3: Assessing and permitting data use (HDAB)

The HDAB assesses the application/request and evaluates whether it meets legal and ethical standards and whether it aligns with one of the permitted purposes under the EHDS. If approved, it then notifies the HDU of the estimated fees and, upon acceptance of that estimate, the HDAB issues a legally binding data permit, which outlines the scope of use, conditions, and obligations of the HDU.

Step 4: Providing the data (HDH)

Upon approval, the HDAB notifies the relevant HDH(s). The HDH has three months to provide the specified dataset to the HDAB for processing. The final fees for the HDH must be agreed upon and itemised within one month of permit approval and if they can't come to an agreement the health data access body may set the fees. In the event that a disagreement continues, the HDH or HDU shall have access to dispute settlement bodies.

Step 5: Preparing and curating the data (HDAB)

This is a critical function of the HDAB. Upon receiving the data, the HDAB is responsible for preparing it for the HDU. This can involve:

- Standardising and formatting the data
- Applying pseudonymisation or full anonymisation
- Removing data from individuals who have opted out
- Combining the data (data linkage) or other curation services

Step 6: Analysing the data in a Secure Processing Environment (SPE) (HDU)

In case of a data permit, the HDAB makes the prepared data available to the HDU exclusively within a SPE. The SPE must include:

1. Secure hardware and long-term storage
2. Analytics tools
3. Cybersecurity and privacy controls

Crucially, the HDU cannot download any personal data from the SPE. Only aggregated, non-identifiable results can be exported.

The HDU must only analyse the data within the HDAB's SPE and can only analyse the data requested and purpose defined in the data permit.

Step 7: Publication of results (HDU)

For a Health Data Access Application (and Health Data Request), the HDU must publish the results within 18 months, inform the HDAB of the results, and must mention that the results have been obtained by using data in the framework of the EHDS.

HDABs are responsible for:

- Publishing permits and applications/requests, and links to outputs
- Closing the SPE and deleting data within 6 months of the permit's end
- Notifying affected individuals if significant findings arise from the research

Multi-country data requests

Multi-country health data access is coordinated through the central services, HealthData@EU, which hosts a Union-wide data catalogue, a common data access application/request form and enables data exchange between national HDABs. Each Member State appoints a national contact point (typically within the HDAB) to route applications and requests, coordinate responses, and facilitate secure access. Once permits are issued, data is accessed via national or EU-level SPE (EHDS Frequently Asked Questions). See figure 6 for the steps involved in in the reuse of multi-country health data under EHDS.

Figure 7: Steps involved in the reuse of multi-country health data under EHDS

Data discovery via HealthData@EU catalogue	To help users identify datasets across Member States, the European Commission maintains a federated, Union-wide dataset catalogue including the national and Union catalogues.
Unified application submission	Multi-country applications (and requests) can be submitted to an individual HDAB in the Member State of the applicant, of the HDH, or to HealthData@EU, specifying the purpose and datasets needed from multiple countries.
Application routing via national contact points	HealthData@EU automatically forwards the application to the relevant HDAB responsible for receiving EU-level data applications, coordinating the national input and response.
HDAB review and cooperation	HDABs assess the part of the application relevant to their jurisdiction. HealthData@EU provides tools for cooperation between HDABs, including platforms to share information such as conditions applied.
Data permit issuance	Each HDAB either grants or denies a data permit. Decisions are communicated to the applicant through a lead HDAB or via the HealthData@EU interface.
Analysis in a Secure Processing Environments (SPE)	The Commission will, upon request of the HDABs, provide an SPE to make data available for analysis.
Transparency and oversight	HDABs publish summaries of permit decisions and the HDU publishes the results. The EHDS Board and the European Commission provide oversight to ensure legal consistency.

Table 2. Key deadlines for health data access applications and requests

ACTION/PROCESS	TIMELINE
Decision on application	• The HDAB has 3 months (extendable by up to 3 months) to issue or refuse a data permit/ request from receipt of a complete application • A public sector applicant may request an accelerated procedure of 2 months (extendible by up to 1 month) • Trusted Health Data Holders have 2 months, before the HDABs have 2 further months, to review those decisions
Agreement of fees	• The fees should be estimated by HDH and shared with HDAB and HDU prior to the permit being granted, then agreed between the HDU and HDH within one month after granting the permit
Provision of data to HDAB	• The HDH has 3 months from receipt of the request (extendable by up to 3 months) to provide the HDAB with the data
Provision of data to user in a secure processing environment	• The HDAB has 2 months to make data available after receiving it from the HDH • For data requests, the statistical analysis should be provided within 3 months (non-binding) from the acceptance of the request, including the time it takes for the HDH to provide the data
Data analysis	• The HDU has up to 10 years to conduct the analysis, depending on the permit
Data deletion	• Data in the secure environment must be deleted within 6 months after the permit expires
Publication of results	• The HDU must make results public within 18 months of completing data processing (can be extended)

Case Study: Findata — Finland's centralised health data permit authority

Though the EHDS is the first cross-national data sharing system, similar initiatives have already been implemented in the EU. The closest parallel is Findata, the Finnish Health and Social Data Permit Authority, which provides a useful case study for how the EHDS is likely to operate.

Operational model

Established in 2019, Findata functions as a centralised Health Data Access Body (HDAB), streamlining the secondary use of health data for research, development, innovation, and policy-making. Findata has a narrower scope of health data and health data holders than the EHDS, is limited to Finnish data.

Findata operates as a one-stop-shop for data permit applications, coordinating with multiple data controllers to facilitate access to pseudonymised or anonymised datasets. It provides Secure Processing Environments (SPEs), where approved users can analyse data without downloading or transferring it externally. This model ensures compliance with GDPR and national legislation, and in the future, EHDS.

Findata's responsibilities include:

- Evaluating applications for secondary data use
- Coordinating data extraction, combination and preparation with data controllers (health data holders)
- Ensuring data minimisation and privacy protection
- Providing access to data exclusively within the SPE

Application volume

In 2024, Findata received **316 applications**, including:

- Data permit applications: 34%
- Data permit amendment applications: 54%
- Statistical data requests (equivalent to EHDS data requests): 8%

The number of applications has increased from over 250 in 2021.

On average, one permit covered data from more than four different data controllers.

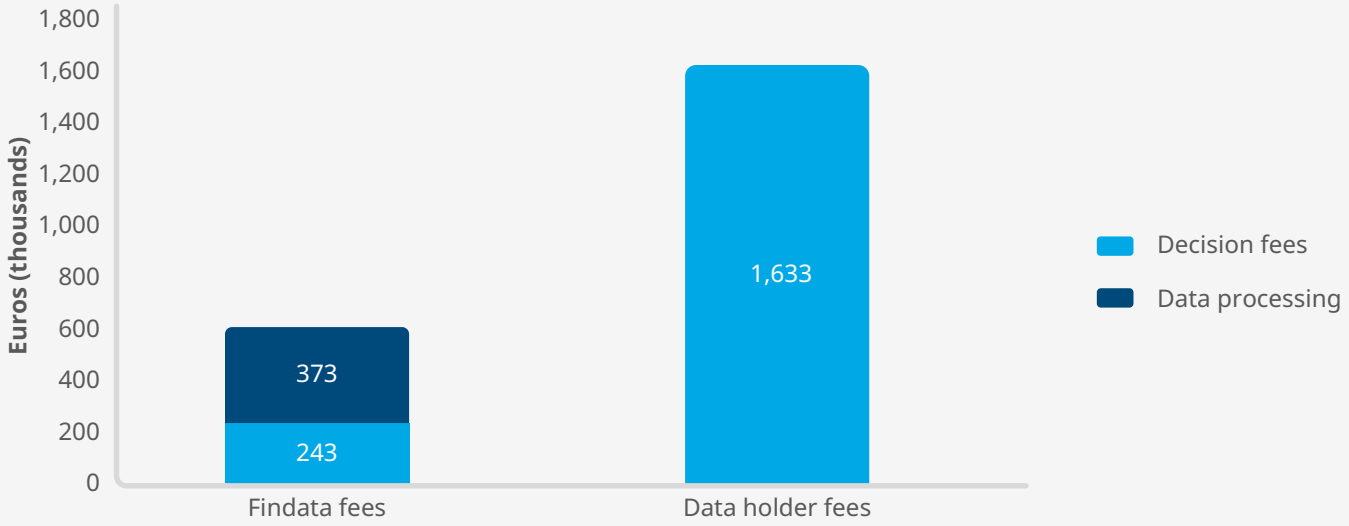
In 2024, Findata ran 131 consultations to support applicants with personalised advice — something missing from the EHDS legal text but likely to be crucial.

Costing and efficiency

Findata's pricing model is transparent and based on processing costs.

In 2024 the average cost per application was €1,600 (Median cost: €700). See figure 8

Figure 8. Fees charged by Findata's decision and processing fees and data extraction costs charged by controllers



Source: Findata annual report 2024

The data permit applications were processed in a median of 82 days, with two thirds of that time spent waiting for information from the applicant or data holder.

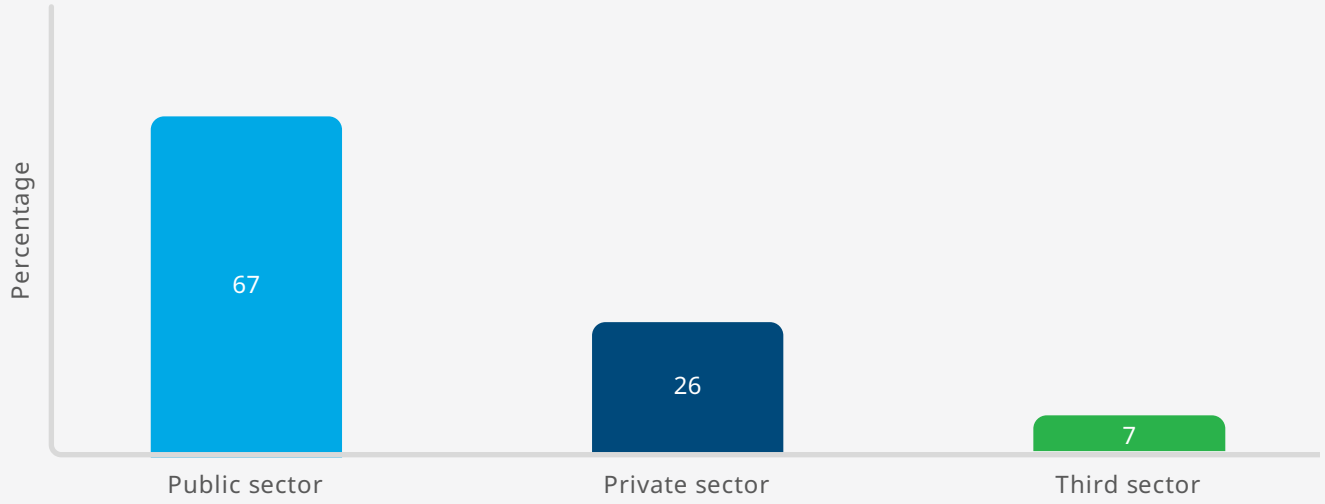
Organisational structure

Findata employs approximately **20 staff members** and has an annual budget of around **€2.5 million**, including EU funding for strategic initiatives such as **FinHITS**, a project aimed at harmonising health data infrastructure across Finland.

Applicant breakdown

Applications to Findata come from a diverse range of sectors (Figure 9):

Figure 9. Applicant stakeholder types in 2024



Source: Findata annual report 2024

This distribution highlights the broad utility of health data across academia, industry, and civil society.

Types of applications

Findata processes applications for:

- Scientific research (92%)
- Statistical analysis (6%)
- Development and innovation (2%)
- Other (<1%)

Challenges

Despite its success, Findata faces several operational challenges:

- **Delays due to GDPR requests:** Findata experienced significant service delays in mid-2024 due to a surge in citizens exercising their GDPR rights. Opt-out volumes are something the EHDS will seek to manage through Member States establishing their own system
- **Data quality errors** in the health data have led to announcements and may have affected multiple HDUs. This is a problem for all data reuse and will be a problem in the EHDS
- **Powerful enough secure processing environments** to handle large databases and volume of users. Does not support the growing number of users, handle very large datasets, or utilize advanced methods

Findata provides a useful benchmark for the level of EHDS demand, the reuse motivations and the likely challenges HDABs will face.

Health Data Holders (HDHs)

Across the European Union, countless organisations will be classified as Health Data Holders. HDHs are defined in the legislation as any entity that is the controller of personal electronic health data, or can make health data available through the control of the technical design of a product and related services. This includes hospitals, research institutions, public bodies, pharmaceutical companies, pharmacies, GP practices etc. However, organisations with fewer than 10 employees and an annual turnover or balance sheet below €2 million are excluded.

Under the EHDS, HDHs have an obligation to hand over their data upon receiving a request from their national HDAB. HDHs are required to make the following categories of data available for secondary use per EHDS Article 51:

- Electronic Health Records
- Data impacting on health, including social, environmental behavioural determinants of health
- Relevant pathogen genomic data, impacting on human health
- Health-related administrative data, including claims and reimbursement data
- Human genetic, genomic and proteomic data
- Person generated electronic health data, including medical devices, wellness
- Applications or other digital health applications
- Identification data related to health professionals involved in the treatment of a natural person
- Population wide health data registries (public health registries)
- Electronic health data from medical registries for specific diseases
- Electronic health data from clinical trials
- Electronic health data from medical devices and from registries for medicinal products and medical devices
- Research cohorts, questionnaires and surveys related to health
- Electronic health data from biobanks and dedicated databases
- Electronic data related to insurance status, professional status, education, lifestyle, wellness and behaviour data relevant to health
- Electronic health data containing various improvements such as correction, annotation, enrichment received by the data holder following a processing based on a data permit

Key requirements for Health Data Holders

HDHs will have to begin registering their data with the HDAB starting from March 26th, 2029, and subsequently ensure these descriptions are updated annually. The EU Commission will, by means of Delegated Acts, publish the content and format requirements for the dataset descriptions by March 26th, 2027.

Making your data public: By 2029, HDHs will need to catalogue their health data in the National Catalogues.

- **Identify your data sets and their metadata.** They also have the option of providing an additional 'Data Quality and Utility Labels' to their data. The latter is mandatory for publicly funded data bases and includes:
  - **Data documentation:** Metadata, supporting documents, data dictionary, format/standards, source, (if applicable) data model
  - **Technical quality:** Completeness, uniqueness, accuracy, validity, timeliness, consistency
  - **Data quality management:** Maturity of processes (review, audit), bias examination
  - **Coverage:** Period, population, (if applicable) representativity, average time for individual appearance
  - **Access and provision:** Time from collection to dataset, time to provide data after approval
  - **Data modifications:** Merging, adding data (including links)

Additionally, if your dataset is protected by intellectual property rights or trade secrets, it is essential to document and disclose this information. This ensures that the HDAB considers these rights during its assessment of the health applicant's request and implements appropriate technical and organisational measures to safeguard these rights if a permit is granted.

- **Upload and maintain the metadata in the National Data Catalogue** of the HDAB in the country your organisation operates in or where you hold the data. Maintenance of your metadata needs to be done at least once a year

Supplying your data on demand: Provide data upon request from HDABs in accordance with the format and structure specified in the national health data catalogues. Ensure timely delivery of data within three months to HDABs. HDHs are expected to implement internal controls to ensure no unauthorised data is included.

Note: non-compliance with the EHDS results in proportionate penalties for HDHs, which will be monitored by HDABs per EHDS Article 63.

Trusted Health Data Holder: Member States can designate certain HDHs as "trusted" if they meet criteria such as having their own secure processing environment and the expertise to assess data requests or applications. For requests or applications involving only data from a trusted HDH, the trusted HDH can perform the initial assessment and propose a decision to the HDAB, streamlining the process significantly. The HDAB retains oversight and accountability for each application decision.

Challenges for Health Data Holders

Below are key challenges HDHs may encounter. The subsequent section will outline potential solutions to each of these challenges.

OVERARCHING CHALLENGES:

- **Financing the change:** For HDHs, particularly those who have little experience and capacity in the secondary use of health data, the new obligations represent a significant additional responsibility. They will need support, guidance, and adequate financial compensation to manage their new responsibilities for data cataloguing and provision. So far, there is no clear provision for compensation to prepare for EHDS2, which will be decided on by each Member State

- **Motivating the change:** Given the benefits of providing periodic metadata and source data for reuse are only indirect, motivating staff for compliance may be challenging
- **EHDS timelines versus capacity:** the HDH needs to provide the data within maximum lead times which requires capacity and capability but the frequency and scope of requests is unclear, making resource planning to meet the EHDS responsibilities challenging, especially for organization which do not have specific or allocatable data management capacity and capabilities

REGISTERING YOUR DATA AND MAINTAINING YOUR METADATA IN THE NATIONAL CATALOGUE:

- **Gathering all data assets ("data mapping"):** Many HDHs (e.g., hospitals or research institutions) have legacy data systems. Some data might not be easily discoverable or documented. Therefore, there is a potential challenge related to redundant data entry across fragmented systems. This data may not easily be accessible for reuse
- **Updating metadata:** A potential challenge for HDHs may be ensuring tight-knit coordination between updates in the dataset and updates in their catalogue data. Misalignment could lead to HDHs working with outdated or misleading information
- **Registration effort vs actual reuse of your data:** the HDH has the obligation to upload and maintain its metadata in the National Catalogue but its reuse is not guaranteed. HDHs needs to have the discipline to continue their maintenance efforts

SUPPLYING YOUR DATA ON DEMAND:

- **Cross-functional coordination:** Supplying data on demand may be made more difficult if the data is coming from multiple units or departments in your organisation, particularly when each likely has different accountability structures. Some data sources may be difficult to retrieve the appropriate data from, requiring special expertise
- **Responsibility for data minimisation:** HDHs are expected to follow the data minimisation principles under General Data Protection Regulation (GDPR): that data is adequate, limited to what is necessary and relevant. But it is unclear to what extent this applies to the data they provide to HDABs under EHDS
- **Expectations of data use for improvement:** If HDHs are expected to be ready to provide their data on demand, it is likely that they will spend resources keeping their registered data up to date internally. However, there may be cases in which the newly maintained internal data will reveal risks in their operations (e.g., a hospital's newly pulled data reveals previously undetected below the benchmark rates of neonatal hypothermia post-operatively). There is an ethical and legal obligation to address these risks, particularly safety risks, once they are known, which will require even more HDH resources in the form of improvement specialists
- **Recording the costs of making this data available:** This is especially hard to track and prove in organisations which do not for example log hourly time or record activities consistently
- **Resources:** Not all HDHs have the capacity and capabilities to provide (extract, including data minimization if the request concerns personal health data, and send) the requested data to the HDAB in time

Recommendations for Health Data Holders

The following section outlines recommendations for HDHs in response to the example challenges above. This section is not intended to be comprehensive but rather illustrate.

REGISTERING YOUR DATA:

- **Prepare to identify and catalogue all health data assets** that fall under the scope of the EHDS. Understand their format, standards, and quality, especially regarding standardised labelling and formatting. If possible, consider assigning named 'data stewards' for key domains (e.g., oncology, cardiology) to lead local data mapping efforts and promote accountability
- **Prepare for the obligation to register your data** in the National Catalogue in the format and scope required by the HDAB. Establish internal processes for continuously creating, validating, and at a minimum annually updating the required metadata.
- **Identify the health data that is protected** by Intellectual Property Rights, trade secrets, or Regulatory Data Protection, for example, clinical trials. HDHs can inform the HDAB about these protections and may suggest safeguards to protect their reuse, though it is the HDAB that determines whether the data warrants protection and what protection
- **Start educating and informing your staff** about EHDS, focussing on the what and why of EHDS: the new legal responsibilities, what data reuse is, what's in it for us and most importantly what needs to be done to be compliant as per March 2029

ENGAGING WITH HDABS:

- **Participate in HDAB decision making** as soon as your national HDAB is designated to shape and negotiate practical guidelines on responsibilities, network topology, data formats, compensation, and quality standards, and get clarity on what implementation is are required by when as well as what support is available
- **Create a data minimisation template** to standardise practice around what is meant by the "minimum necessary" standard and recognise cases where data minimisation is unlikely to work effectively

SUPPLYING YOUR DATA ON DEMAND:

- **Evaluate your capacity and capability** to extract and transfer (large) datasets to the HDAB, upon request and the capabilities needed to record the costs to make the data available. Consider the resources and timeframes required and identify potential bottlenecks. If needed, consider working with a data intermediation entity which will take on your EHDS responsibilities
- **Establish a multi-functional EHDS team** that includes data and legal/compliance expertise to coordinate the handling of EHDS requests. This should ensure responsibilities and processes across different functional areas are rehearsed

Health Data Access Bodies (HDABs)

HDABS are national authorities responsible for managing access to health data for secondary use. Member States may have more than one HDAB, but one 'coordinating' HDAB needs to be designated to ensure the HDABS are able to deliver on the key requirements below.

Key requirements for Health Data Access Bodies

An operating model to deliver the below requirements is set out in Appendix 3.

ESTABLISHING EHDS

- **Building and maintaining the National Data Catalogue:** HDABs will need to establish an online, standardized catalogue of health datasets and their characteristics which will be populated by HDHs. The metadata will be based on an EC implementing act, informed by TEHDAS, and include the option of HDH's completing a 'data quality and utility label'
- **Designing a fee structure:** HDABs need to create fair and consistent pricing models for data access and processing, for themselves, including if an application or request is withdrawn. They may also provide guidance for HDH on fees. Fee-agreements should be concluded between the HDH and HDU, within 1 month after data permit and may need an itemized breakdown. In certain cases, HDABs may facilitate negotiations between the HDH and the HDU
- **Setting an application and request process:** HDABs will need to establish an application protocol detailing the steps HDUs need to take, and a system to manage the applications. Both will be harmonized between HDABs by TEHDAS. To run them will require application processing software
- **Offering Secure Processing Environments (SPEs),** HDABs will need to provide data access via secure, auditable, and user-friendly Secure Processing Environments. The SPE must comply with certain security measures, such as ensuring that authorised access is only granted to electronic health data covered by the data permit, keeping identifiable logs of all activities, and monitoring potential security threats, such as nonpermitted download of data. This will require:
  - » Hardware, including adequate long-term storage
  - » Software, including data analytics tools
  - » Cybersecurity and privacy measures
  - » May include payable-addons, such as additional software, hardware or services

RUNNING EHDS

- **Issuing permits and agreeing on fees and Intellectual Property protections:** Once an application is approved, a permit must be granted to the HDU requesting the data. Concurrently, the HDH's fees and any applicable intellectual property protections for the data should be requested, such as minimising data provision
- **Data processing:** HDABs must implement robust processes to assess, standardise, remove non-relevant data (data minimisation), remove opt-outs (as per EHDS Article 71), (pseudo)anonymise and any other optional additional services. This must be done within two months. For Data Requests, HDABs need to establish capabilities to process, analyse and provide anonymised statistical data

- **Establishing trust and compliance:** HDABs are responsible for a range of legal requirements, including but not limited to, purpose limitation and the granting of special protections, such as for IP and trade secret protection, enforcing an HDH's failure to populate the catalogue, and checking the catalogue is accurate and up to date

  HDABs must oversee that the HDU uses the data for the purposes under the permit only and does not download it. They also need to ensure IP and trade secret protections and check that the HDU has published the results appropriately (within 18 months)

  A big part of ensuring trust and compliance is communication. For HDHs in particular, HDABs need to make sure that they are aware of their requirements and how to fulfil them

- **Publishing and notifying:** issued data permits and data requests must be published on the (coordinating) HDAB website. Natural persons must also be notified of any significant finding from the research related to them

- **EHDS maintenance:** HDABs will need to conduct audits. Collaborate with other HDABs, the EHDS Board, ethics committees, and data protection authorities via HealthData@EU. Share best practices, harmonise permit procedures and technical standards, and support consistent EU-wide implementation

INVOLVEMENT IN NATIONAL LEGISLATION

HDABs may be involved in drafting national legislation in the following areas:

- **Expansion of Health Data Holder definition:** Member States have the option to extend the obligations placed on Health Data Holders to natural persons and microenterprises

- **Health data intermediation entities:** National law may specify that the duties of certain categories of Health Data Holders can be carried out by designated Health Data Intermediation Entities

- **Additional data categories and stricter safeguards:** Member States can legislate to make additional categories of electronic health data available for secondary use. Furthermore, they may introduce stricter measures and additional safeguards at the national level to protect particularly sensitive data, such as genetic, epigenomic, and genomic data

- **Exceptions to the right to opt-out:** National law may provide for a mechanism to override a natural person's opt-out for specific, important reasons of public interest, such as for activities carried out by public sector bodies to protect against serious cross-border health threats or for scientific research. Any such national law must provide for "specific and suitable measures" to protect the fundamental rights and personal data of natural persons

Challenges for Health Data Access Bodies

Below are example challenges HDABs may encounter, beyond the difficulties of setting up a new operating model and organisation. This section is not intended to be comprehensive but rather illustrate. The subsequent section will outline potential solutions to each of these challenges.

RESOURCING:

- **Hiring the right skill mix:** HDABs must interpret and enforce complex legal protections (e.g., IP, trade secrets, and purpose limitation) and processes (e.g., what applications are and are not approved; opt out procedures). They will also need to ensure that they have the skills needed to process a multitude of different data types

- **Sustainable financing of the HDAB**
- **Handling finances:** Particularly if there is a need to deal with financial commitments from HDUs and interim loans to HDHs
- **Designing a 'fair' fee structure:** The EHDS allows HDHs to charge fees for data access to cover their costs. However, it may be challenging to agree fee structures applicable to HDHs of various types (e.g., for-profit versus non-profit). Furthermore, different national or organisational cost structures may lead to significant variation, creating equity concerns among HDHs operating across borders

PROCESS AND STAKEHOLDER CHALLENGES:

- **Training HDH and HDUs:** HDABs will need to train the users of EHDS to meet their requirements along all aspects of the user journey
- **Evolving HDU requests:** As research evolves, HDUs may need to adjust their permit terms. This isn't foreseen in the EHDS

DATA QUALITY AND PROCESSING CHALLENGES:

- **Difficulty processing poor quality data:** Because data and metadata are registered by HDHs themselves, often without independent validation, HDABs may face challenges in processing unstandardised data
- **Substantive data processing:** To meet EHDS deadlines, HDABs must efficiently process the data which includes pseudonymisation, linking, and opt-out handling and may require standardisation. Additionally, combining and anonymising might sometimes be impossible for heterogeneous databases

GOVERNANCE AND STANDARDS CHALLENGES:

- **Setting consistent standards:** HDABs may also be involved in national laws on HDH exemptions, however, national interpretations may vary, creating inconsistent enforcement across the EU (e.g., what counts as sufficiently anonymised or protected; what data is and isn't available). Additionally, changing national priorities, decentralised decision making, or lack of shared precedents may contribute to inconsistency between and within HDABs
- **HDHs "cherry picking" the data registered:** HDHs will have different data. Therefore, mandating that certain types of data are submitted across all HDHs may be challenging. However, if the decision of what to register is left to the HDHs themselves, HDHs are unlikely to invest more time and resources in registering their assets than required, particularly in hospitals with legacy systems that will require significant manual entry
- **Balancing SPE security and user-friendliness:** Ensuring its security against breaches while making it user-friendly is a major technical challenge given that common features for data security (e.g., restricted access to few HDU professionals) may lead to expected workarounds (e.g., HDU professionals providing screenshots to colleagues)
- **Balancing enforcement and support:** HDABs will need to strike a delicate balance between penalising non-compliant HDHs/HDUs and helping them meet standards. An overly punitive approach could drive strict compliance with the requirements but may also minimise the extent to which they use the EHDS and go beyond the basic requirements. Too lenient an approach risks misuse
- **Lagging legal and technical information:** the EHDS regulation provides frameworks but has regulatory gaps, and technical details are missing, including:
  - » A uniform opt-out interface
  - » Specialised software for more efficient metadata labelling
  - » Standardised methods for conducting tests
  - » Details of a 'trusted open public database' that is to be established by the Commission. There is currently no clarity
  - » The process and power HDABs have for informing policy amendments if the current system is not feasible

Recommendations for Health Data Access Bodies

The following section outlines recommendations for the HDABs in response to the challenges above. In many cases, the recommendations will need to be bespoke and implementation support may be needed.

ESTABLISHING EHDS:

- **Plan for the recruitment and training of multidisciplinary teams** with expertise in skills ranging from IP law to data science. Consider whether to build all capabilities in-house or to partner with external experts
- **Learn from existing fee structures:** Consider adapting pricing structures from existing national health databases that grant permits for secondary use. For example, under Finland's Health Data Permit Authority (Findata), Findata charges for permits, data preparation, data extraction, and specialised access to the SPE
- **Publish a tiered, transparent fee structure,** which includes clear withdrawal fee policies, to help HDUs anticipate costs and support equity across diverse applicant types (non-profit, public, commercial)

- **For the National Data Catalogue use metadata validation scripts and alerts** to flag metadata inconsistencies, missing fields, or version control issues to improve catalogue reliability without manual checking
- **Build resilient infrastructure,** particularly the data catalogue and SPE. The volume and complexity of data applications and requests will grow over time, and your systems must be able to adapt. Format standardisation and storage space are key considerations in this regard
- **Incentivise quality contributions** to recognise HDHs that go beyond minimum metadata or data quality through e.g. through recognition or league tables. This will promote voluntary improvement without requiring punitive measures
- **Cross HDAB collaboration:** work together across the Member States to share best practices and the financial and resource burden. For example, to co-design, implement and maintain technology like the DAAMS, the catalogue and web portals, and most importantly work towards a consistent HDU experience across the EU region
- **Prioritise HDH, HDU, and citizen stakeholder engagement:**
  - » Clear communication about the benefits of EHDS data reuse and the robustness of privacy safeguards is essential to minimise opt-out rates. This includes creating accessible educational materials, addressing misconceptions, and establishing channels for citizens to provide feedback and raise concerns
  - » From the outset, consistently ask for user feedback to design a system that is practical, trusted, and meets user needs

RUNNING EHDS:

- **Develop a living precedent library** to internally track decisions related to ambiguous cases (e.g., opt-outs with partially anonymised data) to build institutional memory and consistency and reduce ad hoc interpretation. AI can be a useful tool here
- **Establish a feasibility 'triage' process and offer feasibility reviews** to minimise issues down the line, such as data quality flaws. IQVIA has found that a large percentage of data reuse studies that seem possible on paper turn out to be unfeasible in reality without early feasibility assessment. This assessment may involve direct communication with HDUs or collaborating with HDHs to assess the feasibility before committing to a full EHDS application
- **Require transparent reporting** of evolving findings from HDUs. Mandate that the rationale for both the original permit and iterative permits are reported to establish an audit trail
- **Feedback:** For the SPE, HDABs should include feedback mechanisms that address problems

Health Data Users (HDUs)

Health Data Users are the people or organisations seeking to use health data for secondary purposes.

Key requirements for Health Data Users

- **Ensuring compliant data requests and applications:** Before any request/application is made, the health data applicants are required to ensure a lawful basis for data use under GDPR and EHDS. Article 54 outlines prohibited purposes for secondary data use, which include, but not limited to, advertising to healthcare professionals, developing products which are harmful to individuals
- **Pay fees:** have the funds to pay the agreed-upon fees of HDABs and HDHs. Whilst these fees will be limited to the costs of processing and providing the requested data, they could be substantive in some cases. Fees need to be paid as of the start of the application process
- **Using the data appropriately:** Ensure those accessing and using the data within the designated SPE only do so in line with the approved data permit and do not share data with unauthorised third parties
- **Notifying significant findings related to an individual's health:** HDUs must inform the HDAB of any significant finding related to the health of the natural person whose data are included in the dataset
- **Publishing results:** Publish results of secondary use within 18 months and report findings to HDABs, citing the EHDS

Challenges for Health Data Users

Below are example challenges HDUs may encounter. This section is not intended to be comprehensive but rather illustrate. The subsequent section will outline potential recommendations to each of these challenges.

ESTABLISHING COMPLIANCE READINESS:

- **Consequences of non-compliance:** HDUs need to have a clear understanding of consequences that come with non-compliance. Major infringements can be subject to €20 million or 4% of the preceding annual turnover respectively, alongside bans on EHDS use for up to 5 years

PREPARING THE APPLICATION OR REQUEST PROCESS:

- **Risk of applying for data that later proves unsuitable:** The EHDS workflow does not include a formal feasibility assessment step before a full data access permit is approved. This creates a risk that HDUs will invest in an application only to discover later that the data is not suitable for their research question. This "usefulness gap" could lead to inefficiencies, failed projects and unnecessary fees paid
- **Working within EHDS timelines and the data permit.** The unpredictable and potentially extendable timeline of EHDS may make it challenging to use within normal research funding cycles
- **Predefining a purpose which may change:** HDUs must predefine their research purpose in detail and may not deviate after approval. This restricts exploratory or iterative research that may not align with real-world study timelines or academic norms
- **Transparency,** all data permits and requests will be published by the HDAB, and the results of the data analysis must be published by the HDU
- **Fit for purpose,** the current version of the regulation doesn't enforce any interoperability standards, which could add insurmountable complexity of the data analytics and/or the necessity of HDH support. This could lead to extended lead times or even termination of the research

USING SPES:

- **SPE suitability for required analysis:** HDUs must conduct analyses within national or EU-level SPEs, which may lack software/hardware computational capacity, capability, and analysis needs. Additionally, the SPE may reduce the feasibility of cross-sectoral linkages (e.g., with environmental or socioeconomic data)

PUBLISHING RESULTS:

- **Data submission pressure:** HDUs are required to publish within 18 months and report findings. This can be particularly challenging if unforeseen barriers arise or if the findings from the research are unexpected and require further analysis

Recommendations for Health Data Users

The following section outlines recommendations for HDUs in response to the example challenges above. This section is not intended to be comprehensive but rather illustrate.

ESTABLISHING COMPLIANCE READINESS:

- **Develop internal EHDS compliance playbooks** that cover each stage of EHDS participation (e.g., application writing, SPE use, publication). This will minimise re-creating processes for each application/request and will institutionalise knowledge, which will be particularly useful for rotating staff or cross-border collaborations

PREPARING THE REQUEST OR APPLICATION PROCESS:

- **Build sample analysis models** to estimate how useful the data will be before applying. This will ensure the investment of applying and waiting for the data will be worthwhile. Furthermore, applicants/HDUs could set up a subnetwork of preferred HDH's whose data and data structure they understand, limiting the chance of failure
- **If possible, request pre-submission consultations with HDABs/HDH** to validate feasibility or dataset relevance. HDABs or HDUs may be able to provide early feedback and align expectations
- **Establish an internal SPE readiness sandbox** for 'heavy users' of EHDS to mimic key constraints of standard SPE features and specify the analytic tools that will be needed in the data application. Alongside investment in staff training to familiarise themselves with these new environments, this may also ensure compatibility with the computational resources available in SPEs
- **Have your say** in the set up of the network by engaging with the HDABs to help built a network, processes, templates, etc. which are useable from a data user point of view

PUBLISHING RESULTS:

- **Implement an internal EHDS publication tracker** to monitor timelines for each EHDS project, including data access date, analysis milestones, and publication deadline. Sharing this timeline early with institutional ethics committees or legal teams will facilitate on time completion or, in the case of delays, provide evidence for a defensible case for requesting extensions
- **Leverage the extension clause** if needed (Article 61 (4). HDUs may ask for additional time if they can adequately justify it, especially for publishing purposes

Readiness checklist

The below section contains a selection of key questions HDHs, HDABs, and HDUs should consider understanding their readiness gaps. Although these may not be urgent, given the EHDS2 implementation timeline, they are worth thinking about in advance.

Health Data Holders (HDHs)

PEOPLE	PROCESS	TECHNOLOGY
• Do we have the capacity and capability to take on the EHDS tasks and responsibilities (see column Process and Technology)? • Can we estimate how often data requests will be issued and with that forecast the workload?	• How will we create and maintain metadata entries? • Who is responsible for validating metadata before submission? • How do we appropriately extract data, prepare them for sending and send them? • How do we respond to data quality issues being surfaced by our data being reused? • How do we provide support, and quantify the costs of this support, if it is requested or required by applicants or the HDAB? • How do we protect our IPR, trade secrets, or regulatory data protection? • How do we properly apply "data minimization" in case personal identifiable data is to be shared with the HDAB?	• Do we have the (secure) infrastructure and solutions in place to extract and send the requested data? • Do we have the solutions to perform de-identification and opt-out?

Health Data Access Bodies (HDABs)

PEOPLE	PROCESS	TECHNOLOGY
• Do we have a business case to hire staff (in advance)? • Do we have a flexible resource pool to manage fluctuating demands and still remain within the legal timelines? • Do we have a knowledge management system to ensure consistency over time and across staff/HDABS and facilitate continuous learning? • Do we have the advisory capability to create and maintain the local legal framework? • Do we have the capability to assess applications related to all the 17 data categories mentioned in Article 51, and all use cases in Articles 53 and 54? • Do we have the technical capacity and capability to support the HDU with the SPE and the analytical tools provided in it?	• How will we coordinate with other HDABs? • How will we ensure compliance in all its aspects? For example, the Secure Processing Environment (SPE) is both auditable and secure while still being usable; the use of the health data is in line with the data permit etc. • How will we triage data access applications/ requests to meet EHDS timelines? Which consistent and evolving assessment criteria will we apply and enforce? • How will we ensure that the national network is useable, feasible and sustainable, and remains as such? • How do we educate our staff to take on the variety HDAB tasks? And how do we keep that capability up to par to meet the legal requirements? • How will we set up and maintain the local data network (e.g. central, federated or hybrid network topology, encourage FAIR principles)? • How do we enforce and monitor the GDPR principles like data minimization and de-identification? • How do we set up a feasible, acceptable, consistent and transparent fee structure?	• Do we have a user-friendly DAAMS-tool to support the data application process end-to-end? • Do we have a back-office system supporting transparency and traceability? • Do we have the tools to link, curate, de-identify and opt-out data? • Do we have the tools to connect to the EC central services? • Do we have the budget to invest in technology? Do we collaborate to relieve the investment, operational and maintenance burden? • Which analytical platforms will we provide in the SPE?

Health Data Users (HDUs)

PEOPLE	PROCESS	TECHNOLOGY
• Have we properly educated our staff in how to operate and comply with EHDS2?	• How do we ensure our EHDS2 compliance? Do we have specific processes in place to support? • How do we forecast the fees and timelines before entering the formal application process? • How do we ensure that the data selected in the catalogue are fit for purpose before entering the (costly) application process and data use? • How will we know if the data we are requesting will meet our needs? • How do we instruct the HDAB to set up a proper SPE? • How will we manage multi-country projects? • How do we align with the HDAB to feedback on practical issues we encounter (e.g., usability, data gaps, SPE friction)?	• Can we use the analytical platform(s) provided by the HDAB?

Conclusion

The European Health Data Space (EHDS) marks a pivotal evolution in the EU's digital and health strategy, harmonising fragmented health data policy into a unified, operational framework. By enabling the secure and ethical re-use of electronic health data, the EHDS aims to transform how data is accessed and reused for care, research, and innovation across Europe.

As the regulation moves toward implementation, the scale of its ambition becomes clearer. Yet the path to realising these benefits is complex. Real success depends on moving beyond compliance. The EHDS should be seen as a strategic opportunity, not a burden, to build a future-ready, data-rich health ecosystem. Public-private partnerships, including the involvement of experienced actors like IQVIA, will be essential in designing and delivering the technical, legal, and operational components required.

The EHDS is Europe's opportunity to set a global benchmark for responsible, secure, and impactful use of health data. If implemented boldly and inclusively, it can serve as a lasting catalyst for health transformation, delivering better outcomes for patients, strengthening research and innovation, and building more resilient and equitable health systems across the EU.

How IQVIA can help?

As organisations across Europe prepare for the transformative requirements of the European Health Data Space (EHDS), IQVIA and Privacy Analytics are supporting stakeholders with a comprehensive, privacy-first approach. Leveraging deep expertise in health data reuse, governance, regulatory compliance, and advanced privacy-enhancing technologies, IQVIA helps governments, health data access bodies, and data holders navigate the complexities of EHDS implementation. Our solutions are designed to unlock the full value of health data for research, innovation, and policy, while ensuring robust protection of patient privacy and adherence to EU standards. Below are key ways IQVIA can help your organisation succeed under EHDS:

1. STRATEGIC GUIDANCE AND IMPLEMENTATION SUPPORT

IQVIA offers deep expertise in designing, building, and operating EHDS-compliant infrastructure for governments and health data access bodies (HDABs). This includes:

- **Governance and operating models:** IQVIA can help define governance structures, stakeholder engagement models, and operational workflows tailored to national and EU requirements

- **Regulatory alignment:** Leveraging experience with GDPR, EHDS, and other EU frameworks, IQVIA ensures compliance while enabling innovation

2. NATIONAL DATA CATALOGUES AND DATA MANAGEMENT

- **Catalogue design and management:** IQVIA has proven experience in creating and maintaining large-scale data catalogues, such as its work with the European Medicines Agency (EMA). This expertise can be directly applied to help HDABs build and maintain their National Data Catalogues, ensuring robust metadata, data quality, and utility labelling
- **Data mapping and stewardship:** IQVIA supports Health Data Holders (HDHs) in identifying, cataloguing, and preparing their data assets for secondary use, including guidance on metadata, technical quality, and compliance with EHDS standards

3. PRIVACY-ENHANCING TECHNOLOGY AND SECURE PROCESSING ENVIRONMENTS

- **Privacy analytics platform:** The Privacy Analytics Platform provides scalable, defensible anonymisation solutions that meet global standards (GDPR, HIPAA), and can be integrated with existing systems from local pilots to national programmes
- **Secure Processing Environments (SPEs):** IQVIA delivers sophisticated, rule-based anonymisation and auditing solutions, exemplified by the privacy-enhancing technology layer for NHS England's Federated Data Platform (FDP). This enables secure, scalable data use across millions of patient records, with automated de-identification, audit trails, and privacy controls

4. CONSULTING AND ADVISORY SERVICES

- **Gap assessment and road mapping:** Privacy Analytics experts help organisations assess current data governance, identify gaps, and design a roadmap for EHDS compliance and innovation
- **Stakeholder engagement:** IQVIA supports HDABs and HDHs in stakeholder engagement, change management, and training, ensuring trust and compliance from the outset

5. REAL-WORLD DEPLOYMENTS AND CASE STUDIES

- **NHS England FDP:** Core components of the Privacy Analytics Platform power the NHS's Privacy-Enhancing Technology (NHS-PET), enabling secure, scalable data use across 55M+ patient records. Results include reduced waiting times, support for virtual services, and increased hospital throughput
- **Findata (Finland):** IQVIA's benchmarking and consulting draw on lessons from Findata, Finland's centralised health data permit authority, which processes hundreds of secondary use requests annually and provides transparent, efficient data access and SPEs

6. TECHNOLOGY AND PLATFORM INTEGRATION

- **Flexible integration:** The Privacy Analytics Platform is designed to integrate seamlessly with existing health data systems, supporting interoperability, scalability, and compliance across diverse environments
- **Automation and auditability:** Automated data transformation, de-identification, and audit trails ensure responsible data use for research, innovation, and service planning

7. CONTINUOUS IMPROVEMENT AND FUTURE READINESS

- **Monitoring regulatory updates:** IQVIA provides ongoing support to help organisations stay up to date with evolving EHDS requirements, Delegated Acts, and technical specifications
- **Public-private partnerships:** IQVIA is positioned as a strategic partner for governments and health systems, supporting the design and delivery of technical, legal, and operational components required for EHDS success

Should you want to hear more about how IQVIA can help implementing EHDS, email info@iqvia.com

Staying up to date

Given the evolving nature of EHDS, it is important to stay tuned for the latest updates:

- European Health Data Space
- Towards the European Health Data Space – TEHDAS2
- Extended EHR@EU
- Privacy Analytics EHDS Webpages

Feel free to reach out to IQVIA as info@iqvia.com who will be happy to help you keep up to date.

Appendix 1: Difference between primary use and secondary use

Primary use: Primary use refers to the processing of personal electronic health data for the purpose of providing healthcare to individuals. This includes the access, sharing, and updating of health data by healthcare professionals to support diagnosis, treatment, and continuity of care across the EU.

MyHealth@EU is the cross-border digital infrastructure established by the European Commission to enable the secure exchange of personal electronic health data between Member States. Its initial services include access to patient summaries, ePrescriptions, eDispensations, medical images, laboratory results, and discharge reports. To enable seamless data sharing, Member States will be required to make these data categories available in a common European electronic health record exchange format. This will be supported by mandatory requirements for interoperability, security, safety, and privacy, as well as self-certification of electronic health record systems to ensure compliance. Trusted identification systems will further help guarantee secure and consistent cross-border access.

Secondary use: Create a reliable and efficient framework for the use of centralised health data in research, policy, innovation, and regulation. This is the focus of this white paper and represents the most significant shift for research and innovation.

Permitted purposes for secondary use include:

- Scientific research in health and wellbeing
- Development and innovation activities for new products or services.
- Training artificial intelligence algorithms.
- Providing personalised healthcare.
- Informing public health policy and regulatory decisions

Health data holders will make the following categories of electronic health data available:

- Electronic health data
- Data related to socioeconomic, environmental, behavioural determinants of health
- Registry data (public health, mortality, medical registries)
- Administrative data (dispensations, reimbursements)
- Aggregated data on healthcare needs, resources allocated to healthcare, access to and provision of healthcare, healthcare expenditure and financing
- Pathogen data related to human health
- Human genetic, epigenomic, and other human molecular or omics data
- Data from wellness apps
- Medical devices data
- Registries for medicinal products and devices
- Data on health professionals' status, specialisation, and institution
- Biobank, cohort, and survey data
- Clinical trial data (certain protections still apply, related to intellectual property rights, regulatory data protection, and trade secrets)

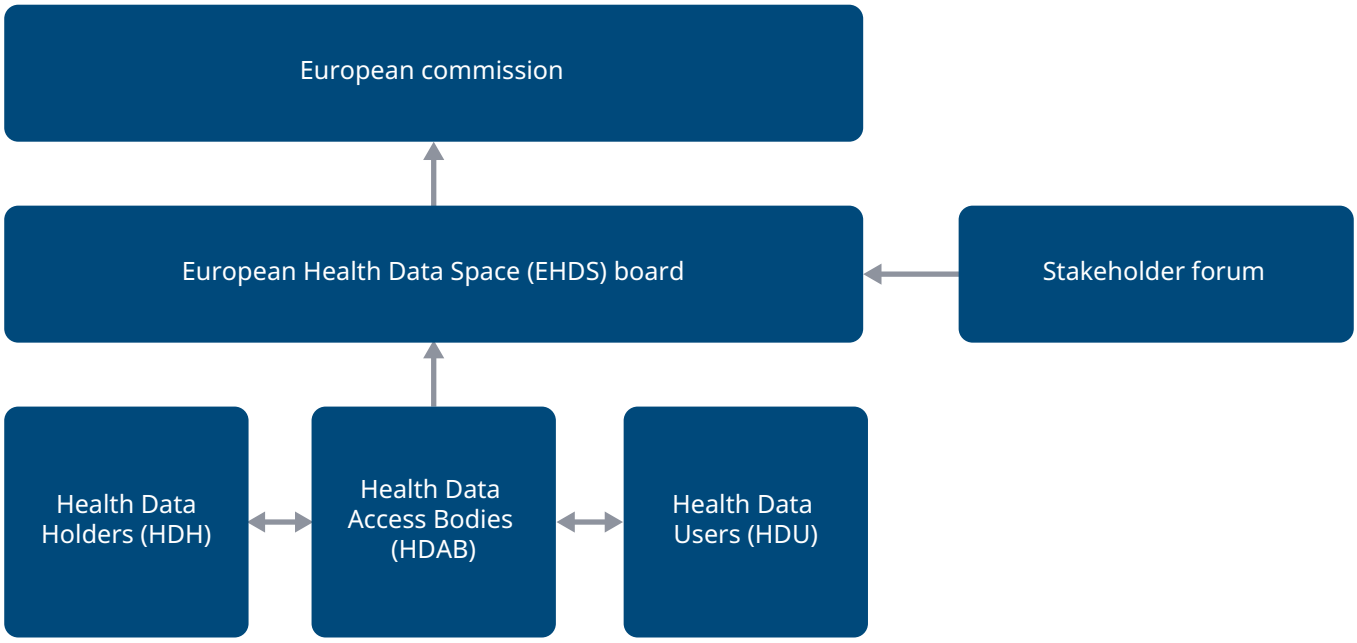
Electronic health data must not be used for:

- Decision-making that harms or discriminates against individuals (e.g. insurance or employment)
- Marketing and advertising
- Creating harmful products (e.g. addictive or illicit goods)
- Any activity that breaches national ethical laws

Appendix 2: The proposed governance structure

The EHDS framework is built upon a multi-layered governance structure involving both EU-level and national bodies (See Figure 3)

Figure 10. EHDS2 Governance Structure



The European Commission: Provides policy leadership by proposing and enforcing EHDS Regulation and issuing guidance. Key responsibilities will include:

- **Developing and maintaining EHDS standards and specifications**
- **Operating a central platform** for secure cross-border data exchange and an EU-wide data catalogue linking national HDAB catalogues
- **Maintaining a public register of data users and permits** to align EHDS implementation with EU laws, notably the General Data Protection Regulation (GDPR)
- **Setting harmonised data access fees,** and possibly model data-sharing contracts and enforcement guidelines in collaboration with the EHDS Board, which it chairs

The EHDS Board: The EHDS Board, co-chaired by the European Commission and a Member State representative, will include national HDAB and data protection authority representatives. It will advise the Commission. Key responsibilities will include:

- **Facilitating cooperation** among Member States and the Commission
- **Coordinating implementation practices** for digital health authorities (EHDS1) and HDABS (EHDS2)
- **Creating subgroups** to address specific issues

Stakeholder forum: Chaired by the European Commission, it serves as a consultative platform for a wide range of stakeholders including representatives of patient organisations, health professionals, industry, consumer organisations, scientific researchers and academia. Key responsibilities will include:

- **Organising and leading** forum meetings
- **Establishing subgroups** to address specific technical or policy issues
- **Facilitating exchanges** between the Stakeholder Forum and the EHDS Board

The operational success of the EHDS, particularly for the secondary use of data, hinges on developing new infrastructure and a trio of key stakeholders:

1. **HDHs** (Health Data Holders) (e.g., hospitals, registries, research institutes)
2. **HDABs** (Health Data Access Bodies) (e.g., national authorities granting access to data)
3. **(applicant) HDUs** (Health Data Users) (e.g., researchers, companies, and public bodies using the data)

Appendix 3: Operating model of the Health Data Access Body

With the European Health Data Space (EHDS) Regulation entering into force on 26 March 2025, the foundation has been laid for a unified European framework for the secondary use of health data. Within this framework, Health Data Access Bodies (HDABs) play a pivotal role: they are responsible for assessing data access applications, processing health data, ensuring legal and ethical compliance, and enabling secure data analysis. The complexity of this role is significant, driven by the diversity of tasks and responsibilities HDABs must fulfil — ranging from legal review to technical data exchange and compliance oversight.

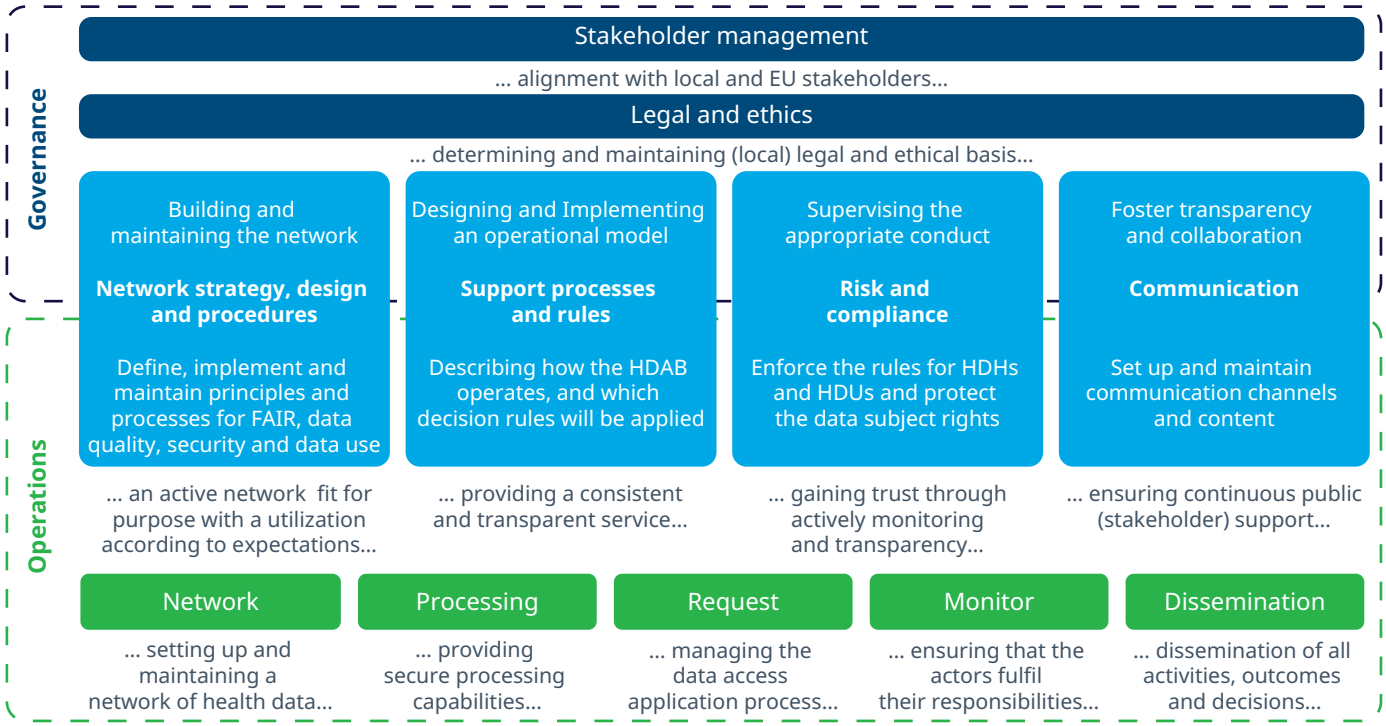
To manage this complexity and guide implementation, a clear and widely supported operating model is essential. This model serves as a reference framework for structuring processes, decision-making, and collaboration with external parties. It makes strategic choices explicit and ensures consistency in execution. Crucially, the operating model must not only be aligned internally but also actively communicated to Health Data Holders (HDHs). They need clarity on expectations, procedures, and how to prepare for their role within the EHDS network.

The timeline adds urgency: implementation begins in March 2027, and by March 2029 HDABs must be fully operational for nearly all data categories. This means the coming period should be used to define, align, and communicate the operating model. Moreover, a degree of uniformity across Member States is highly desirable to improve the user experience for Health Data Users, particularly in the context of cross-border secondary use, where consistency in procedures and expectations will be key to enabling seamless access and collaboration.

OPERATING MODEL OVERVIEW:
An operating model defines how an organisation is structured and functions to deliver on its objectives.
It translates strategic intent into practical capabilities by outlining key roles, processes, and governance arrangements. For Health Data Access Bodies (HDABs) under the European Health Data Space (EHDS) Regulation, the operating model provides a coherent framework for fulfilling their responsibilities in enabling the secondary use of health data.

The HDAB operating model ensures that all core functions — from stakeholder engagement and legal compliance to data processing and oversight — are aligned and integrated. It supports consistent execution, transparency, and accountability, while offering clarity to external partners such as Health Data Holders (HDHs) and Health Data Users (HDUs).

Figure 11: The tasks and responsibilities of a HDAB divided into governance and operational aspects



The model is structured around two complementary layers: Governance and Operations.

The Governance layer provides strategic direction and oversight. It encompasses leadership structures such as governing boards or steering committees, which set objectives, approve major initiatives, and monitor performance. Governance ensures that HDABs operate in line with EHDS goals and national health data strategies, and that they remain accountable to public authorities and stakeholders. It plays a critical role in steering the organisation through evolving regulatory and operational landscapes.

The Operations layer covers the day-to-day delivery of HDAB services. It includes managing resources, IT systems, workflows, and stakeholder interactions to ensure timely and compliant execution of tasks. This layer translates strategic decisions into practice. Effective operations are essential for meeting legal timelines, maintaining service quality, and ensuring a seamless experience for all actors involved.

THE 11 BUSINESS FUNCTIONS:

1. Stakeholder management

Ensures alignment with local and EU stakeholders through structured engagement and collaboration. Builds trust and support by maintaining open dialogue and adapting to stakeholder needs.

2. Legal and ethics

Establishes and maintains the legal and ethical basis for HDAB operations. Ensures compliance with EHDS and national regulations, safeguarding data subject rights and public trust.

3. Network strategy, design and procedures

Defines the technical and procedural framework for connecting with Health Data Holders and Users. Encourages FAIR data, quality, security, and interoperability to support a robust and reliable network.

4. Support processes and rules

Outlines internal procedures and decision-making criteria for consistent and transparent operations. Enables scalability and clarity across HDAB activities through documented protocols.

5. Risk and compliance

Monitors adherence to EHDS rules and enforces compliance among all actors. Protects data subjects by identifying risks and applying corrective measures when necessary.

6. Communication

Manages public and stakeholder-facing communication channels and content. Promotes transparency and understanding of HDAB activities, decisions, and services.

7. Network (Operational execution)

Executes the delivery of approved health data by coordinating extraction, transformation, and secure transfer. Ensures data is provided accurately, securely, and in line with EHDS standards.

8. Processing

Operates the Secure Processing Environment (SPE) for authorised data analysis. Prepares and curates data from Health Data Holders, ensuring privacy and compliance throughout.

9. Request

Handles the full lifecycle of health data access applications. Evaluates, approves, and manages requests to ensure fair, timely, and compliant access to data.

10. Monitor

Continuously oversees the fulfilment of responsibilities by HDAB, HDHs, and HDUs. Identifies gaps in performance and initiates follow-up actions to maintain system integrity.

11. Dissemination

Shares outcomes, decisions, and insights from HDAB activities. Enhances transparency and maximises the value of secondary data use through public reporting and knowledge exchange.

CONTACT US

iqvia.com