M6.1 Guideline for health data holders on making personal and non-personal electronic health data available for reuse.

TEHDAS2 – Second Joint Action Towards the European Health Data Space

7 September 2025

Co-funded by the European Union

0 Document info

0.1 Authors

Lead Author(s)	Lead organisation
Marije van Melle	Nictiz (NL)
Rob Schubert	Nictiz (NL)
Maria Athanasaki	GRNET (GR)
Federico Banchelli	RER (IT)
Beatriz Barros	Sciensano (BE)
Elena Berti	RER (IT)
(Asimina) Boupaki	Ministry of Health (GR)
Kristina Bränd Persson	NBHW (SE)
Rasmus Elrud	NBHW (SE)
Silvia Ghiselli	RER (IT)
Joel Granwald	NBHW (SE)
Zdenek Gütter	MZCR (CZ)
Lucija Raic	CIPH (HR)
Jessica Zamberletti	RER (IT)

0.2 Keywords

Keywords	TEHDAS2, Joint Action, Health Data, European Health Data Space, Data Holder

0.3 Document history

Date	Version	Editor	Change	Status
23-04-2025	0.1		First draft	Draft
16-6-2025	0.3	Peija Haaramo, Coen van Gool, minor task contributors	Revisions according to contributors' and EC review	Draft
1-7-2025	0.4	Published for consortium and EC review	Revisions and layout changes	Draft
07-09-2025	0.5	Published for PSG approval	Revisions and layout changes	Draft
16-9-2025	0.6	Published for Public consultation	Final revisions for public consultation	Final Draft

Accepted in Project Steering Group on 15-09-2025.

Disclaimer

Copyright Notice

List of Abbreviations

Abbreviation	Description
AI	Artificial Intelligence
DAAMS	Data Acquisition, Assessment and Management System
EHDS	European Health Data Space
EU	European Union
GDPR	General Data Protection Regulation
HDAB	Health Data Access Body
HDIE	Health Data Intermediation Entity
LLM	Large Language Models
SPE	Secure Processing Environment
TDH	Trusted Data Holder
TEHDAS2	The second Joint Action Towards the EHDS
TTP	Trusted Third Party

1 Executive summary

This guideline provides practical and operational support to health data holders in fulfilling their role under the European Health Data Space (EHDS) Regulation to make personal and non-personal electronic health data available for secondary use. It focuses on the obligations that apply once a Health Data Access Body (HDAB) issues a data permit or approves a data request.

Health data holders include a wide range of entities – such as healthcare providers, public authorities, research institutions, insurers, and developers of health-related services and devices – that process electronic health data within the minimum categories set out in Article 51 of the EHDS Regulation. Under Article 60, they are legally required to provide the approved data in a timely, secure, and structured manner. This involves interpreting the request, possibly creating a subset with the data described in the data permit or data request approval, applying preparation measures (e.g. pseudonymisation or anonymisation), and providing the data via a Secure Processing Environment (SPE) or other authorised channels, depending on the legal basis and type of data. The guideline distinguishes between flows for personal and non-personal data.

The **legal duties** of health data holders include:

- **Personal Data Provision**: Upon receipt of a data permit or approved request, provide the required personal electronic health data to the HDAB in a timely manner — no later than three months, extendable once by another three months in justified cases (Art. 60(1)). The timeline begins when the HDAB notifies the data holder, in accordance with Article 63(3);
- **Non-Personal Data Provision**: If holding non-personal electronic health data (e.g. anonymised or synthetic datasets, or data not relating to individuals), make such data available via open public databases that comply with standards for transparency, governance, and long-term accessibility (Art. 60(5)); and
- **Dataset Description and Metadata**: Ensure that metadata describing the datasets is submitted to the national dataset catalogue (Art. 60(3)) and reviewed and updated at least once per year (Art. 77(2)).

While not mandated by the Regulation, **TEHDAS2 experts recommend** tasks commonly required for operational readiness and national implementation. These include but are not limited to: organising internal systems for accurate dataset descriptions and quality labels; setting up workflows for data extraction, preparation and secure provision; communicating with HDABs for clarifications, quality checks or complaints; facilitating coordination with other EHDS stakeholders (e.g. SPEs, intermediation entities, pseudonymisation services); correcting errors; and responding to significant findings, which must be communicated under national law (Art. 61(5)).

This guideline will help prepare health data holders to comply with their mandatory obligations and align with national EHDS governance.

This contributes to a harmonised and secure approach to secondary use of health data across Europe. The document forms part of the broader TEHDAS2 deliverables, supporting Member State readiness and consistent EHDS implementation.

2 Introduction and Scope

2.1 Advancing health data use in the European Health Union

As part of the European Health Union, the European Union (EU) is advancing the use of health data for secondary purposes, including research, innovation and policymaking. Smooth and secure access to data will drive the development of new treatments and medicines and optimise resource utilisation, all with the overarching goal of improving the health of citizens across Europe.

TEHDAS2, the second joint action Towards the European Health Data Space (EHDS), represents a significant step forward in this vision. The project will develop guidelines and technical specifications to facilitate smooth cross-border use of health data, and support health data holders (also referred to as data holders within this guideline), data users and the new health data access bodies in fulfilling their responsibilities and obligations outlined in the EHDS Regulation.

TEHDAS2 focuses on several critical aspects of health data use.

- **Data discovery**: findability and availability of health data, ensuring it is accessible for secondary purposes.
- **Data access**: developing harmonised access procedures and establishing standardised approaches for granting data access across Member States.
- **Secure processing environment**: defining technical specifications for environments where sensitive health data can be processed safely.
- **Citizen-centric obligations**: providing guidance on fulfilling obligations to citizens, such as communicating significant research findings that impact their health, informing them about research outcomes and ensuring transparency in how their data is used.
- **Collaboration models**: developing guidance on collaboration and guidelines on fees and penalties as well as third country and international access to data.

TEHDAS2 will contribute to harmonised implementation of the EHDS regulation through the concrete guidelines and technical specifications. Some of these documents and resources will also provide input to implementing acts of the regulation. Hence, the joint action will increase the preparedness for the EHDS implementation and lead to better coordination of Member States' joint efforts towards the secondary use of health data, while also reducing fragmentation in policies and practices related to secondary use.

Work Package 6 has the overarching objective to advance both the common understanding about and the operationalisation of access to electronic health data considering the point of view of different key players along the data lifecycle. M6.1 focuses on providing guidance to health data holders to help them meet their obligations when making both personal and non-personal electronic health data available for secondary use. The target audience of this Guideline are 'health data holders' as defined in the EHDS regulation (Art 2(2) (t)) as: *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, policymaking, 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.

M6.2 Guideline for data users on good application practice for data access and request has developed guidance for data users regarding the requirements and obligations during the application process for data access. M6.3 Guideline for Health Data Access Bodies on the procedures and formats for data access. defines guidance on procedures for HDABs for issuing data permits and decisions on data requests. M6.4 establishes technical specifications and/or requirements for Data Access Application Management Systems (DAAMS).

2.2 Scope and aim

This guideline supports the implementation of the EHDS Regulation by providing practical guidance for health data holders on how to make electronic personal and non-personal health data available for secondary use. It focuses on the health data holders' responsibilities in the data preparation and provision phases that follow the issuance of a data permit or approval of a data request by a HDAB, as defined in Chapter IV of the EHDS regulation.

This guideline is grounded in the obligations established in

- **Article 60 of the EHDS regulation**, which sets out the core duties of health data holders in making data available for secondary use, and
- **Article 63 of the EHDS regulation** which describes the enforcement powers of Health Data Access Bodies with respect to health data holders.

The scope of this guideline includes:

- The roles and responsibilities of health data holders in the secondary use pathway within the EHDS infrastructure for secondary use;
- The processes for preparing and providing data, including understanding and interpreting the permit or request, extracting, preparing and transferring the relevant data to a Secure Processing Environment (SPE);
- Communication protocols and procedural interactions between the health data holder, the HDAB, and other actors during data preparation and provision.

To ensure consistency across the Joint Action, this guideline focuses strictly on the logistical, procedural, and organisational aspects of data provision. Several important dimensions are addressed in detail in other TEHDAS2 work packages, and are therefore not elaborated further in this document, including:

- Dataset description (including metadata provision) and dataset catalogue obligations, addressed in M5.1.1 Guideline for health data holders on data description, describing the data holders' duties regarding data description on Data discovery.
- Opt-out management, citizen information and rights – addressed in M8.1 Guideline for Health Data Access Bodies on implementing opt-out from the secondary use of health data and, M8.2 Guideline for Health Data Access Bodies on implementing the obligation of notifying the natural person on a significant finding from the secondary use of health data, and M8.3 Draft guideline for Health Data Access Bodies on informing natural persons about the use of health data – "Citizen Information Point";
- Data anonymisation, pseudonymisation, and linkage techniques – addressed in M7.2 Technical specification for Health Data Access Bodies on data minimisation and de-identification, and M7.5 Guideline for Health Data Access Bodies on linkage of health datasets.

For specific linking with the other TEHDAS2 work packages see Annex 6 Data holder resources.

While these elements are essential for the full implementation of the EHDS framework, this document focuses on helping health data holders understand and fulfil:

- core duties related to responding to HDAB requests and providing data securely, efficiently, and in compliance with the conditions set out in data permits or approved data requests;
- additional optional or recommended tasks TEHDAS2 experts foresee that are implied by the EHDS regulation's related articles (described in Annex 2 Links to the EHDS regulation).

The overall aim of this Guideline is to:

- provide guidance to health data holders on their core duties under the EHDS regulation, with a focus on data preparation and data provision following a data request or permit.
- provide recommendations and illustrative good practice examples based on expert advice and experience.
- support effective communication and coordination with HDABs and other stakeholders involved in the secondary use process.
- help health data holders and Member States to prepare for the implementation of the EHDS, to guide health data holders in fulfilling their role and duties under the EHDS

when making health data available for secondary use. These actors may hold personal and/or non-personal health data and have responsibilities defined under the Regulation.

- help data holders assess their readiness and prepare accordingly. While the Regulation defines a common set of duties in Article 60, the current degree of preparedness and national implementation capacity will vary. Member States are expected to establish supporting governance structures and infrastructure to facilitate compliance.

In order to support consistent interpretation, this Guideline distinguishes between mandatory obligations, recommended practices, and elements left to the discretion of Member States. Formatting cues or a structured typology (for example *[MANDATORY under EHDS]*, *[RECOMMENDED], [EXPERT ADVICE] or [GOOD PRACTICE]*) may be used to highlight these differences. Tasks that are implied by the EHDS-text or reflect expert opinion or best practices, should be considered recommended rather than binding. Illustrative examples are provided throughout the document to support implementation, but these are not prescriptive, as Member States may adopt different approaches depending on their national context and governance structures.

2.3 Target audience/ intended users

This document is primarily aimed at health data holders, who are responsible for making their datasets available in accordance with the EHDS regulation. The definition of 'health data holder' is described in Article 2 (2)(t) of the EHDS regulation, and can include a wide range of entities, such as:

- Healthcare providers (e.g., hospitals, clinics, and general practitioners)
- Public authorities or agencies involved in health or care services
- Health insurances and organisations managing reimbursement systems
- Developers of health-related products and services, including wellness applications
- Research institutions and mortality registries
- EU institutions, bodies, and agencies that manage or process health data.

These entities process personal or non-personal health data and are responsible for ensuring that their datasets are properly described and shared with HDABs. This guideline outlines the key roles and responsibilities of health data holders concerning the secondary use of data under EHDS. It emphasises critical topics that data holders must understand and address to comply with these duties.

Besides the health data holder, other stakeholders within the EHDS institutional landscape can benefit from these guidelines.

- It will serve the HDABs in making them understand the data holders' mandated duties and recommended or optional tasks, and to help prepare for the possible interactions that can be expected in all phases of the user journey. To facilitate these interactions,

Member States should ensure that clear, secure, and traceable communication channels are established as part of the national EHDS infrastructure.

- Furthermore, this guideline will inform the work of the Member States and the European Commission regarding the data holders' mandated duties and recommended or optional tasks, and to help prepare the national EHDS governance and infrastructure as well as the central services set up by the EU.

3 Legal obligations of health data holders under the EHDS regulation

To support implementation of the EHDS regulation, health data holders across Member States must prepare to fulfil their duties related to the secondary use of health data. These obligations apply regardless of a provider's legal status (public or private) or financing model. Article 60(1) makes no distinction between public and private entities and public and private health services, unless an exemption applies (e.g. microenterprises).

The health data holders targeted by the EHDS regulation are heterogeneous, and the landscape across Europe as well as within Member States is diverse. It should be noted that the EHDS regulation does not distinguish between different healthcare system models, which may define different obligations for e.g. public and private healthcare providers and their associated institutions. There is no differentiation of duties between data holders specialised in collection and curation of databases or registries designed for secondary use, and data holders with other and diverse core businesses. The degree of preparedness and/or capacity for implementation of the EHDS regulation varies and may depend on several factors. While the EHDS outlines a common set of duties for health data holders, it does not prescribe how to fulfil these duties in every possible context and situation. TEHDAS2 guidelines, however, aim to support stakeholders in the initial preparation phase for compliance with the EHDS Regulation.

To facilitate preparation for the EHDS, this chapter aims to provide context and answers to the following questions:

- Who needs to provide data according to the EHDS regulation?
- What are health data holder duties?
- What data needs to be provided and how?
- What do I need to know as a health data holder regarding the EHDS?

3.1 What is a health data holder according to the EHDS regulation

Under Article 2(2)(t) of the EHDS regulation, a health data holder is any natural or legal person, or entity, that processes electronic health data for primary or secondary use.

Health data holders may include:

- Healthcare providers (e.g., hospitals, clinics, general practitioners, physiotherapists).
- Public authorities or agencies involved in health or health care services (e.g. monitoring, statistics, epidemiological surveillance)
- Health insurances and organisations managing care reimbursement systems (e.g. individual payments, benefits).
- Developers of health-related products and services, including wellness applications.
- Research institutions and registries (e.g. health registries, mortality registries).
- EU institutions, bodies, and agencies that manage or process health data.

To avoid disproportionate burden, the EHDS regulation exempts natural persons (e.g., individual researchers) and microenterprises (less than 10 employees and < €2 million turnover or balance sheet) from these obligations by default, unless Member States decide otherwise (see Article 50). See also User guide to the SME definition[1]. If an entity grows and no longer qualifies as a microenterprise, it will become subject to the Regulation. A special situation arises if an enterprise changes its category between a small and a micro enterprise over the years. If such an enterprise has already provided health data in the EHDS (listed in the national metadata catalogue), it is recommended that such an enterprise consider the possibility of continuing to provide the already catalogued data and to maintain and possibly, where relevant, even extend it on a voluntary basis, especially if there was interest in such data among data users. An enterprise that changes its category with respect to obligations set out by Chapter IV of the EHDS regulation should immediately communicate with pertinent HDAB with the aim of finding a suitable solution regarding their health data availability for secondary use. Member States may allow for further availability of the data in question by their national law, for example through intermediation entities.

The obligations of health data holders are laid down in Article 60 of the EHDS regulation. These include duties to respond to data permits or requests, provide metadata, and ensure secure and lawful data transfer to the HDAB or the secure processing environment.

As a data holder within the EHDS organisational landscape, it is essential to understand the role of other stakeholders within the EHDS. Important main roles within the EHDS are:

- The Health Data Access Body (HDAB)
- Health Data Users
- Natural persons

The infrastructure for secondary use of health data may include additional stakeholders and functions that enable data access in various phases, such as data preparation and data provision:

[1] *https://ec.europa.eu/docsroom/documents/42921/attachments/1/translations/en/renditions/native*

- Other data holders, including trusted data holders
- Secure processing environments (SPE)
- Intermediation entities
- Pseudonymisation services
- Trusted Third Parties (TTP)

For clarity on these roles within the EHDS regulation, see the glossary in annex 1 Key Terminology.

3.2 Duties and recommended tasks of health data holders

The main duties of health data holders are defined in Article 60 of the EHDS regulation, with related responsibilities further specified in Articles 66 and 77. These obligations apply to all entities qualifying as data holders under Article 2(19).

The legal duties of health data holders include:

- **Personal Data Provision:** Upon receipt of a data permit or approved request, provide the required personal electronic health data to the Health Data Access Body (HDAB) in a timely manner — no later than three months, extendable once by another three months in justified cases (Art. 60(1) EHDS Regulation). The timeline begins when the HDAB notifies the data holder of the permit or approved request, in accordance with Article 63(3).

- **Non-Personal Data Provision:** If holding non-personal electronic health data (e.g. personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable or synthetic datasets or datasets comprising of data that does not relate to individuals), make such data available via open public databases that comply with standards for transparency, governance, and long-term accessibility (Art. 60(5)).

- **Dataset Description and Data Quality and Utility Label (Metadata):** Ensure that metadata describing the datasets is submitted to the national dataset catalogue (Art. 60(3)) and is reviewed and updated at least once a year (Art. 77(2)).

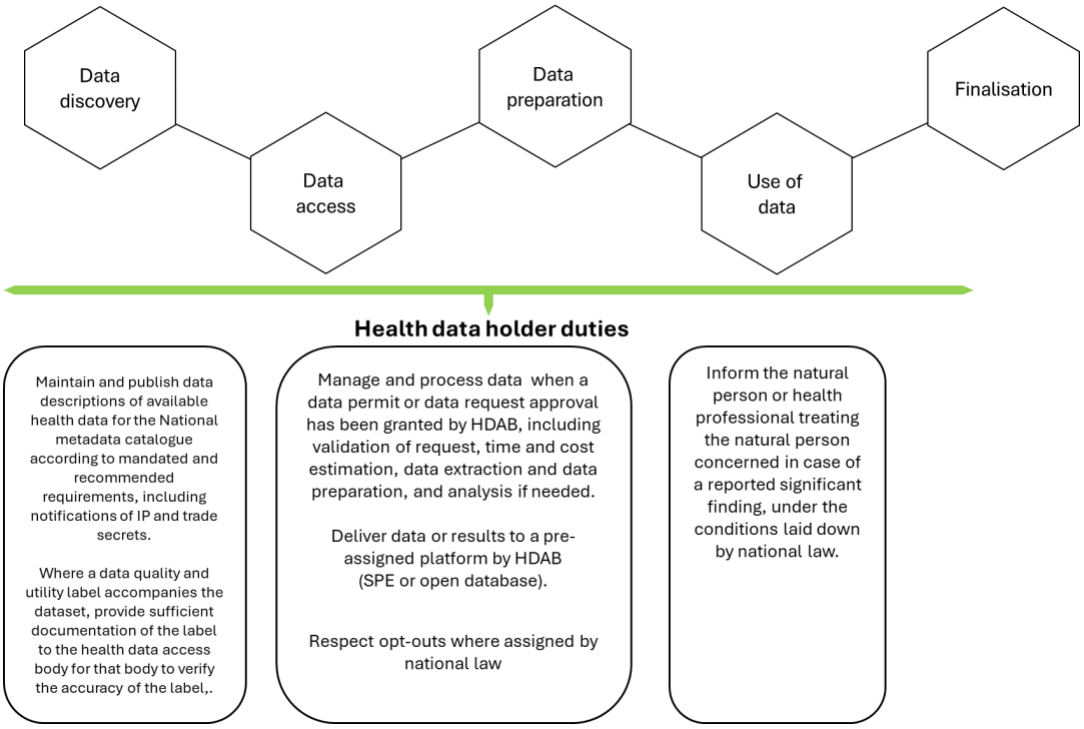
While not mandated by the Regulation, the TEHDAS2 experts advise that these tasks are commonly required to ensure operational readiness and national implementation:

- Organising internal systems and resources to ensure accurate and up-to-date dataset descriptions (including the documentation in case of a data quality and utility label) can be submitted to the Health Data Access Body and integrated in the national dataset catalogue.
- Ensuring internal workflows that can process data requests from the HDAB, including data extraction, data preparation and transfer of data to the designated secure processing environment (SPE) or HDAB.

- Communicate with the HDAB or data users in case of clarifications, quality assurance, or complaints handling (post-delivery).
- Facilitating communication with other stakeholders in the EHDS organisational landscape, such as SPE's, intermediation entities or pseudonymisation services that may be involved in the processing of requests.
- In case when errors are found in the provided datasets are communicated to the data holder, act appropriately so that the error could be fixed. Similarly, but depending on the provisions established by the national law, data holder may be requested to handle datasets that have been enriched by the data users (details are elaborated in D5.4 Short guide for data enrichment for HDABs, data holder and data user).
- Where a health data access body is informed by a health data user of a significant finding related to the health of a natural person, as referred to in Article 61(5) of the EHDS regulation, the health data access body shall inform the health data holder about that finding. The health data holder shall, under the conditions laid down by national law, inform the natural person or health professional treating the natural person concerned.

See Figure 1 below for an overview of the mandatory health data holder duties across the EHDS secondary use process. In this Figure, the duties are linked to the relevant EHDS User Journey phase. For more details on the EHDS User Journey, see Annex 6.4 EHDS Data User Journey.

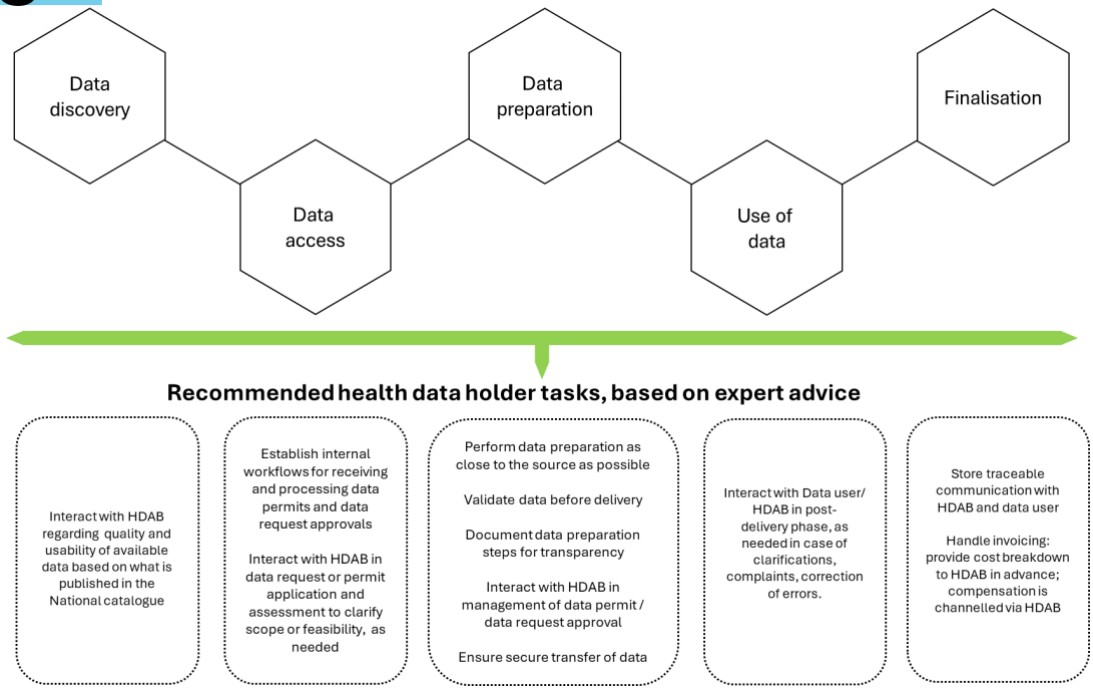
Figure 1 EHDS User Journey and health data holder mandated duties.[2]



In addition, based on the experiences of several organisations and Member States with existing data access and data provision services it is recommended that data holders consider additional expert-advised tasks in conjunction with the interaction points between data users and HDABs along the data user journey. Figure 2 gives some non-exhaustive examples of such recommended facilitation tasks that may be relevant or asked for in different phases of the user journey. For more details on the EHDS User Journey, see Annex 6.4 EHDS Data User Journey.

Figure 2 EHDS User Journey and recommended health data holder tasks, based on expert advice. The tasks in this non-exhaustive list aren't prescribed by the EHDS regulation but recommended. Experts consider these activities good practice.

[2] Trusted data holder status is optional and subject to a number of additional obligations and Member State designation. It is expected that a minority of data holders will qualify and will take up this role.



These are some examples of self-assessment questions for Data Holders. The further investigation of such questions in the particular context of a data holder will help to provide answers, suggested actions and estimated readiness for the EHDS regulation.

Self-assessment: Are You Ready to Provide Data for Secondary Use?

- Which data is in scope and available. How should it be described?
- Which data can be extracted and how to do it efficiently?
- Which non-personal data could safely and effectively be provided as open data?
- Which interactions with HDAB and other stakeholders should we prepare for?
- How do we keep track of data delivered?

3.2.1 The trusted data holder

In addition to general duties under Article 60, the EHDS regulation introduces the possibility for any Member State to decide whether some data holders could be designated as trusted data holders (TDHs), with tasks defined in Article 72(1). Eligibility as TDH requires having the capacity and safeguards to support HDABs by handling certain tasks regarding health data access applications and health data access requests.

Designation process

Designation of trusted data holders is optional, and subject to Member State decision. Member States may establish procedures in their national legislations enabling certain health data holders to apply to be designated as trusted health data holders. Article 72 establishes a simplified procedure for data access via trusted data holders.

To enable this pathway, Member States may designate certain health data holders as TDHs, provided they fulfil all of the following conditions in Article 72(2).

- Ability to provide access to health data through a secure processing environment that is subject to adequate technical and organisational measures and security and interoperability requirements.
- Necessary expertise to assess health data access applications and health data requests.
- Ability to provide the necessary guarantees to ensure compliance with the EHDS regulation provisions for the secondary use of health data, specifically Chapter IV.

Member States shall also establish a procedure to regularly review whether the trusted health data holder continues to fulfil those conditions. Article 72(4) requires a review procedure, but the frequency is left to Member States' discretion

As the EHDS regulation does not mandate the frequency of these reviews, the frequency will be decided by the Member State itself.

Trusted Data Holders must be listed in the national dataset catalogue once approved. Health data holders interested in designation as TDHs should consult their national HDAB or designated authority eligibility and application procedures.

Trusted health data holder duties

Once trusted health data holders have been designated, they may be entrusted at the discretion of the HDAB with performing:

- Preliminary assessment of data access applications.
- Processing and preparation of datasets for permitted access (including pseudonymisation/anonymisation).
- Provision of access to health data through a secure processing environment that complies with Article 73. (Art. 72(2)(a))

The TEHDAS2 experts advise that when a data holder is designated as trusted data holder (Art. 72), they should prepare internal workflows to take on these additional responsibilities.

In accordance with Article 72 EHDS, health data access applications and health data requests shall always be submitted to the HDAB. Where the application only concerns a designated trusted health data holder, the HDAB may forward it to the TDH for assessment.

The TDH may assess whether the criteria for granting the data permit or approving the request are fulfilled and must provide the HDAB with its assessment and a proposal for decision. This must be submitted within two months of receipt of the application from the HDAB. Importantly, the TDH acts under delegation; the HDAB remains the sole decision-maker on whether to issue the data permit or approve the request (Art. 72(4) (5)).

Within another 2 months following the receipt of the assessment, the HDAB shall issue the final decision on the health data access application or health data request. The HDAB is not bound by the proposal submitted by the TDH. While the HDAB may delegate assessments to the TDH, it remains the sole authority responsible for granting or denying access.

The assessment process is described in detail in M6.3 Guideline for Health Data Access Bodies on the procedures and formats for data access and is summarised here.

It is important to note that legally:

- When preparing data or performing anonymisation, the TDH acts as a controller.
- When granting access to the data to a user via a SPE, the TDH acts as a processor on behalf of the user.
- TDHs must store and otherwise process personal health data within the EU, unless an adequacy decision under GDPR applies (Art. 87).

For an illustrative example of a trusted data holder, please see Annex 4 Considerations for implementation.

3.2.2 Health Data Intermediation Entities

To support efficient data provision for secondary use, the EHDS regulation provides the opportunity for Member States to instate national legislation on the appointment of health data intermediation entities (HDIE) which can be used as a tool to reduce the administrative burden on (smaller) health data holders.

These entities may assist certain categories of health data holders, in particular small or less-resourced ones, in carrying out their obligations under the EHDS regulation (see Article 50(3)). Intermediation entities would then interface with the HDAB on behalf of these HDH's, ensuring streamlined data access while maintaining compliance with all regulatory requirements.

When applicable, a HDIE may be required by national law to carry out specific duties *on behalf of* health data holders, for example:

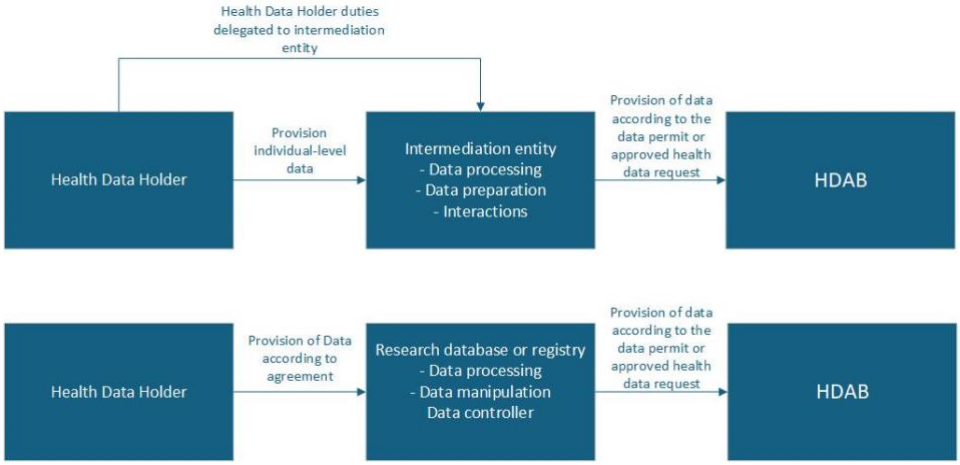
- Preparing and processing data for provision to HDABs.
- Facilitating the submission of metadata to national dataset catalogues.
- Managing technical operations for data sharing.
- Providing access via secure processing environments.

- Enabling compliant data reuse through shared infrastructures.

The roles and tasks of HDIEs may vary between countries and are not standardised at EU level.

Figure 3 provides an illustrative visual example of the delegations of these duties and presents differences with a practical real-life example of a research database (health data holder according to the EHDS).

Figure 3 Delegation of duties to the Health Data Intermediation entity. This is a non-normative, conceptual visual example of delegation via HDIE and the difference with a research database.



Legal Responsibility:
While HDIEs carry out operational tasks, the legal responsibility for compliance with the EHDS regulation remains with the data holder, unless explicitly transferred or defined otherwise in national law. Therefore, health data intermediation entities should not be designated as trusted health data holders.

Example: A Member State designates a public sector body managing a centralised electronic patient records as a health data intermediation entity.

Although the name might be similar, health data intermediation entities under the EHDS Regulation perform tasks that differ from those of data intermediation services under Chapter III of the Data Governance Act (DGA). The latter services primarily serve to facilitate voluntary data sharing in a business-to-business context, whereas EHDS intermediation entities act under a public-task framework, supporting compliance with legal obligations to make data available for secondary use.

For an illustrative example of an HDIE, please see Annex 4 Considerations for implementation.

3.3 What data needs to be provided and how?

3.3.1 What is health data in the context of the EHDS regulation?

In the EHDS regulation, Electronic Health Data is defined as: Personal or non-personal electronic health data (EHDS Article 2(2c)). For the purposes of secondary use, Article 51 of the EHDS Regulation sets out the minimum categories of electronic health data that health data holders must make available upon request or permit, in accordance with Chapter IV. These categories include, for example, electronic health records, administrative data related to healthcare, registries, claims, and data from wellness applications. M5.1 Guideline on Data Description provides detailed guidance on how to interpret these categories and identifies typical data holders responsible for each.

3.3.2 Data set descriptions for national dataset catalogue

Health data holders are required to provide a description of the datasets they hold to their HDAB, in accordance with Article 60(3),

This description must be provided in the form of metadata, including details on the source, scope, main characteristics, and conditions for data access (Art. 77). Dataset descriptions must be reviewed for accuracy at least annually. This information is essential to enable health data users to understand the nature and relevance of the available data for secondary use. To support this, the HealthDCAT-AP common metadata model is being fine-tuned and validated in TEHDAS2 for application in the EHDS framework for secondary use, ensuring dataset discoverability and semantic interoperability. The use of HealthDCAT-AP, an application profile based on DCAT and adapted within supportive action preparing the implementation of EHDS, is expected to support implementation of the metadata obligations defined in Article 77 and will likely inform the technical specifications adopted via implementing acts under Article 77(3).

While the legal obligation to provide metadata applies to all relevant data holders, the level of effort required may vary depending on the volume and complexity of data, existing metadata practices, and available expertise. Nevertheless, good-quality metadata can significantly ease future data provision by ensuring better alignment with data requests and facilitating more efficient data extraction processes. Good-quality metadata helps applicants prepare better applications and better descriptions of the data they want, and it is easier for the data holder to provide the data the applicant has requested if its description has been based on the good-quality metadata. Detailed recommendations and non-binding guidance on using HealthDCAT-AP for dataset description, along with further implementation considerations, is available in M5.1.1 Guideline for health data holders on data description, describing the data holders' duties regarding data description on Data discovery.

Importantly, the HealthDCAT-AP common metadata model allows the categorisation of the different types of health data mentioned in the EHDS Regulation:

- **Personal electronic health data [sensitive data]** – if a dataset contains personal electronic health data.
- **Non-personal electronic health data available as non-open data [protected or restricted data]** – if a dataset does not contain any personal electronic health data but is access-controlled.
- **Non-personal electronic health data available as open data [open data]** – if a dataset does not contain any personal electronic health data and is freely available to the public.

This categorisation is important because the three types of data lead to different flows for access under the EHDS framework:

1. Personal electronic health data
   Requires a data permit or data request; provided via the HDAB and processed in an SPE;

2. Non-personal electronic health data – Open Data
   Must be made available via a public platform, in line with Article 60(5), with robust governance and sustainability;

3. Non-personal electronic health data – Restricted Access
   Provided on approval by the HDAB of the data permit or request and may involve additional safeguards (e.g. for commercially sensitive data).

See Chapter 4 (Making data available) for further details on each of these data provision pathways.

Metadata should be complete, accurate and aligned with the actual technical and organisational capabilities of the data holder. Inaccurate or outdated metadata may result in non-compliance with Article 60(3) and Article 77(2)

For further details on description of the data, see the following guidelines:

- M5.1.1 Guidelines for data holders on data description, and
- M5.1.2 Guidelines for HDABs on minimum categories and limitations on the reuse of health data.
- M5.3 Technical Specification on the National Metadata Catalogue, for more details

Under Article 77(1), each HDAB is responsible for maintaining a national dataset catalogue in a publicly accessible and standardised machine-readable format, incorporating the metadata provided by data holders. Finally, under Article 79, these national catalogues are connected to form the EU-level dataset catalogue, which also integrates metadata from authorised participants in HealthData@EU.

Technical and operational requirements for the national dataset catalogue, including metadata management and responsibilities of HDABs, are detailed in M5.3 Technical Specification on the National Metadata Catalogue.

3.3.3 Personal and non-personal data

Under Articles 60(2) and 60(3) of the EHDS Regulation, health data holders must make both personal and non-personal electronic health data available and provide corresponding metadata for inclusion in the national dataset catalogue, where the data falls under the minimum categories listed in Article 51.

What is personal and non-personal data?

Personal and non-personal data is defined in the GDPR regulation as:

- Personal data is defined in Article 4(1) of the GDPR as any information relating to an identified or identifiable natural person.

- Non-personal data is defined in Article 3(1) of Regulation (EU) 2018/1807 as data other than personal data as defined in the GDPR. Non-personal data is "*Data other than personal data as defined in point (1) of Article 4 of Regulation (EU) 2016/679 (GDPR*)".

Non-personal data can have a wide range of characteristics and can, based on their origin, be categorised into:

1. Non-personal data that was originally personal data (personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable)
2. Non-personal data that has never been related to an identified or identifiable natural person
3. Non-personal synthetic data.

The classification of a dataset affects how it is handled, but the obligations to describe and, in some cases, make data available apply to all types. The operational categories are used in TEHDAS2 for illustrative purposes and do not correspond to legal definitions under the EHDS Regulation. Please note that also in case of non-personal data, only data within the scope of Article 51 is within scope.

For illustrative examples, see Annex 4 Considerations for implementation.

Synthetic data

The primary rationale for synthetic data generation in EHDS is privacy protection. Synthetic data can be generated for a variety of reasons, including[3],

[3] Giuffrè, M., Shung, D.L. Harnessing the power of synthetic data in healthcare: innovation, application, and privacy. *npj Digit. Med.* **6**, 186 (2023). https://doi.org/10.1038/s41746-023-00927-3

- Preliminary data exploration: Synthetic data lets recipients explore dataset structure or determine needed variables before accessing real data.
- Code development: Allows coding without using actual personal data, focusing solely on matching data structure (also known as "dummy data").
- Open science practices: Enables sharing code and synthetic datasets openly, facilitating reproducibility and evaluation.
- Educational use: Prevents sharing sensitive personal data with students by providing synthetic examples.

Synthetic data can be generated to mimic personal or non-personal datasets. In the EHDS context, only synthetic data that no longer relates to an identifiable person is considered non-personal and falls under the provisions of Article 60(2).

In M7.2 Guideline on data minimisation, pseudonymisation, anonymisation and synthetic data[4], more details on how to navigate synthetic data in the preparation phase can be found.

3.3.4 Trade secret and intellectual property management

Under the EHDS regulation (Art. 52), health data holders are required to make electronic health data available for secondary use, even when such data encompasses protected intellectual property (IP) and trade secrets (Art. 52(1)). To allow for this, the data holder shall explicitly identify which data are covered by IP rights or other mentioned protected right or for which it deems necessary to protect IP or trade secrets. The data holders must then communicate to the HDAB that their electronic health data contain information covered by IP rights or trade secrets (Art. 52(2)). They may do so when they submit the description of the electronic health data for inclusion in the data catalogue, or subsequently when a permit is issued on or a request approved for such data. In the former case, the use of the “Rights” property within the HealthDCAT-AP common metadata model may be useful to make explicit the presence of data covered by IP and trade secrets. More details on this point can be found in D5.1 “Guideline for data holders on data description”. In any case, the data holder is required to state the reasons that justify the need for specific protection measures of these data (Art. 52(2)), and the HDAB must assess whether the provided justification is valid (Art. 52(3)).

To facilitate the sharing of data protected by IP, it is crucial to develop a set of appropriate protection measures that ensure the protection of the rights of the data holder, while promoting access and use of the data by the data users. In the case of data permits, the HDAB may make the access to personal and non-personal data or pieces of data covered by IP or trade secrets conditional upon the implementation of these safeguarding measures (Art. 52(4)). Pursuant to Article 52(5), the HDAB may deny secondary use of data where a significant risk to IP rights or trade secrets remains, despite the implementation of safeguarding measures.

The safeguarding measures can be included in contractual arrangements between the data holder and the data user (Art. 52(4)), defining restrictions and permissions in proportion to

[4] M7.2 Guideline on data minimisation, pseudonymisation, anonymisation and synthetic data

the degree of protection that needs to be assigned to data covered by IP and trade secrets. Some examples of protection measures that can be implemented are described below. These examples are non-binding and illustrate possible safeguarding measures that HDAB and health data holders may consider, depending on the nature of the data and on the national legal context. They are not explicitly prescribed by the EHDS Regulation.

By way of example and not limited to, these measures can include:

- to add “noise” to data to mask information revealing trade secrets or IP rights, in a way that does not undermine the validity of the data analysis. to grant partial access to the data if the information to be protected emerges from the electronic health data as a whole and not from parts of it.
- to adopt technological tools such as Fully Homomorphic Encryption which allows performing arithmetic and logical operations directly on encrypted data, eliminating the need to decrypt them during calculation and therefore reducing the risk of exposing protected information. Other technological tools that may be useful are Secure Multi-Party Computation or synthetic data.
- to set reciprocal benefit mechanisms between data holder and data user, for example requiring the data user to acknowledge the data holder's fundamental role in contributing to the research. This could include indicating in a contractual agreement that each project or publication resulting from the use of the data includes mandatory citations that acknowledge the data holder's contribution.

In any case, these measures must not compromise the usability of the data for the permitted purposes.

Further guidance is provided in the TEHDAS2 documents M5.1.1 “Guideline for data holders on data description escribing the data holders’ duties regarding data description on Data discovery” and “M6.3 Guideline for Health Data Access Bodies on the procedures and formats for data access”.

3.4 What else do I need to know as a data holder?

This section complements the legal obligations described above by outlining the applicable timelines and cost recovery mechanisms relevant to data holders once a data permit or request has been approved. For organisational readiness aspects (e.g. capability in data management and capacity to take on the duties assigned by the EHDS regulation, technical maturity), see Annex 3.

3.4.1 Timeliness

Upon issuance of a data permit (Art. 68) or approval of a health data request (Art. 69) by the competent HDAB, health data holders are required to provide the requested data within a defined timeframe. Timely data transmission is critical for compliance.

According to Article 60(2) of the EHDS Regulation, data holders must provide the requested data within three months of receiving the data permit or data request. This period may be extended once, for a further three months, in duly justified cases. Where unjustified delays occur, HDABs are empowered to impose enforcement measures, including periodic penalty payments and temporary or permanent restrictions on future data access activities by the non-compliant data holder.

While the EHDS Regulation sets specific deadlines for certain actors, the following timelines illustrate typical durations based on Articles 60, 62, 68–70, and 72:

- In a **data access application**, the HDAB has up to 3 months to issue a permit, the data holder 3 months to provide the data. In justified cases, the health data access body may extend that period by a maximum of three months. The HDAB has another 2 months to share the data in the SPE. The data user then has the duration specified in the permit for analysis, followed by 18 months to publish results.

- In a **data request application**, the HDAB has up to 3 months to asses the request and issue an approval. The data holder has 3 months to provide the data or anonymous statistical output. In justified cases, the health data access body may extend that period by a maximum of three months. The HDAB has 3 months to share the response with the health data user. The data user then has 18 months to publish results.

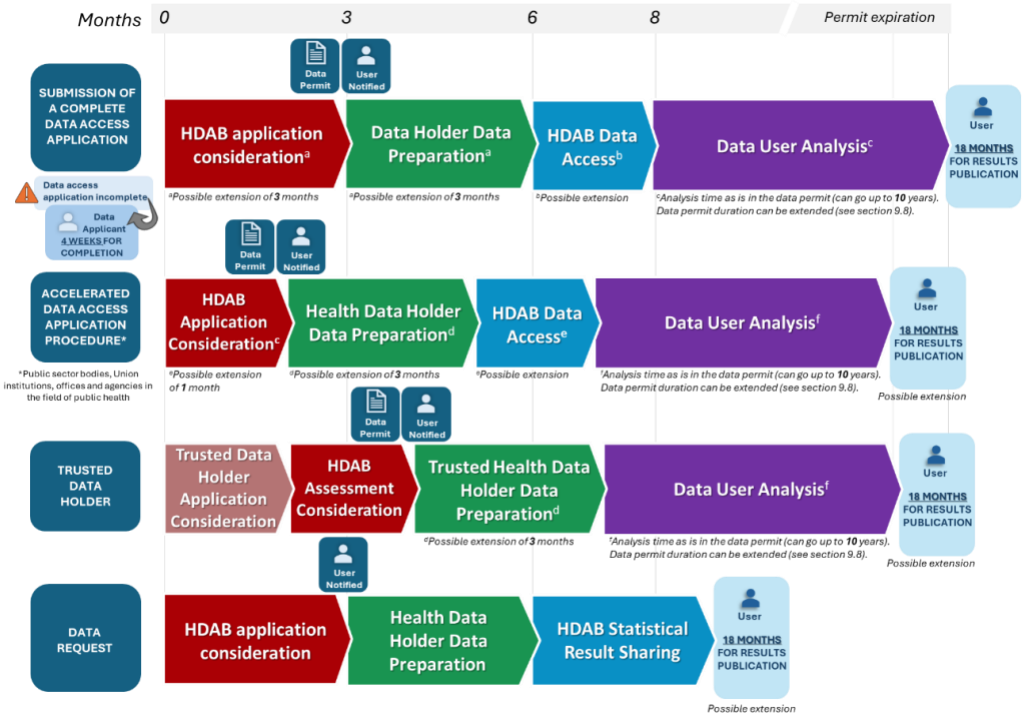
- **Accelerated review** applies to public sector bodies and EU institutions with legal mandates in public health. In these cases, the HDAB must decide within 2 months, though this can extend to 3 months if more time is needed.

- **Trusted data holders** shall assess applications within 2 months and forward their assessment to the HDAB, which has another 2 months for final evaluation. The HDAB is ultimately responsible for the decision and notifying the applicant. This process can take up to 4 months. If approved, the trusted data holder prepares and shares the data on its SPE directly. Data user analysis follows the standard conditions.

Figure 4 presents the timelines for all possible HealthData@EU workflows.

Pursuant to Article 63(7), the HDAB may impose proportionate enforcement measures, including penalties and access restrictions, in cases of unjustified delays or non-compliance.

Figure 4 Different workflows in the EHDS infrastructure for secondary use and their timeframes.[5]



3.4.2 Invoicing, fees and eligible costs

Under Article 62(2), health data holders are entitled to receive compensation for the costs incurred when compiling and preparing electronic health data. These costs are part of the overall fee charged by the HDAB to the data user, and the relevant portion must be transferred to the data holder. The EHDS regulation acknowledges that preparing and transmitting data for secondary use may entail operational costs. Accordingly, Article 62(2) permits health data holders to recover costs for compiling and preparing the data.

Cost estimates must be provided to the HDAB in advance. Eligible costs include data preparation and provision activities, such as data extraction, formatting, or pseudonymisation expenses. Although Article 6 of the Data Governance Act (Regulation (EU) 2022/868) limits fees for reuse of public sector data, it does not apply to health data holders under the EHDS Regulation, including public sector bodies. Cost recovery under Article 62 remains fully applicable. More detail on costing and invoicing can be found in M4.1.1 Guideline on fees related to the EHDS regulation.

[5] Figure derived from TEHDAS2 M6.2 Guideline for data users on good application and access practice

3.5 How to navigate the EHDS landscape and infrastructure

This guideline has outlined and interpreted the legal obligations of a data holder under the EHDS Regulation, and provided practical guidance for their implementation. Next, this guideline will provide guidance on the different paths to walk when making data available. Figure 5 presents an overview of the potential paths when a data permit has been provided and its possible steps and branches depending on key variables, such as the type of data, application type and the potential assignments of intermediation entities. Figure 6 presents an overview of the potential paths when a data request has been approved and its possible steps and branches depending on key variables, such as the type of data, application type and the potential assignments of intermediation entities. Each branch within the flowchart provides guidance on the possible procedural workflows for making data available, depending on the type of data, request, and actors involved. Chapter 5 Data Provision focuses on each of the branches separately.

Having clarified the duties of data holders and the nature of the data to be provided, the following sections will guide through the concrete workflows and interactions involved in making data available under the EHDS framework.

Figure 5 Illustrative workflows for secondary use of electronic health data in case of a data permit. This figure provides a high-level conceptual illustration of the EHDS landscape and infrastructure, showing how data flows may differ depending on specific conditions.
DH=Data holder, HDIE=Health Data Intermediate entities, DU=Data User, Diamond=choices, Box=process, Oval=begin and end point.

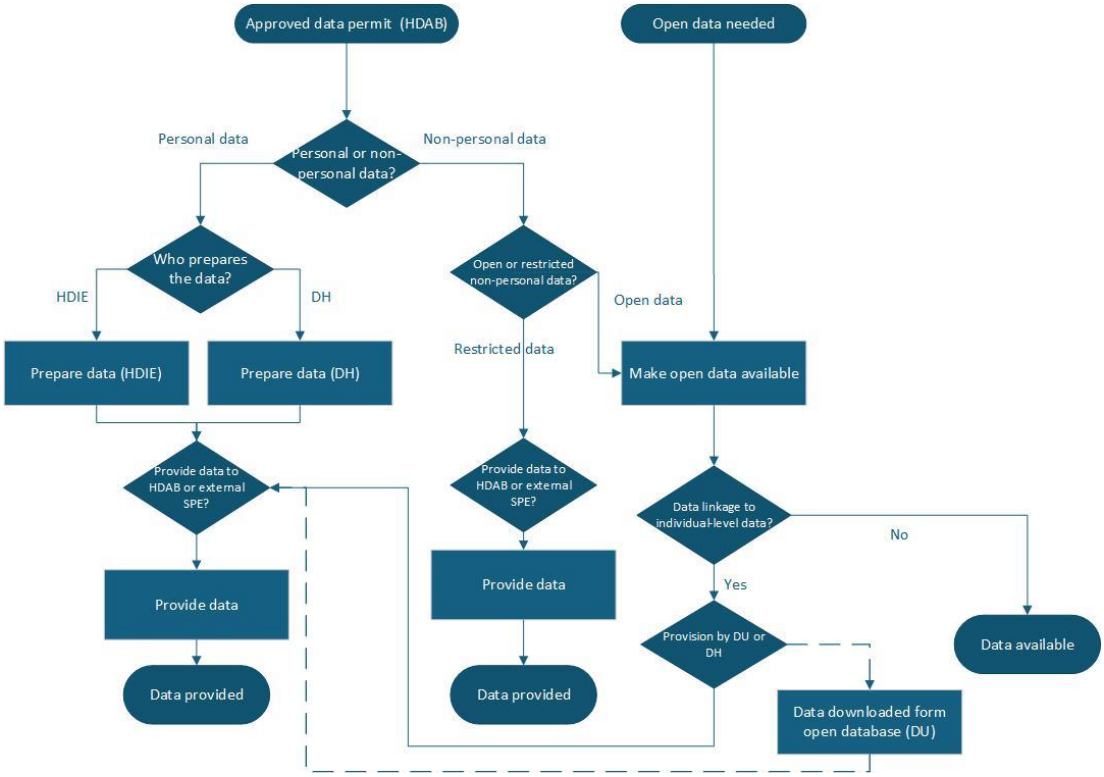
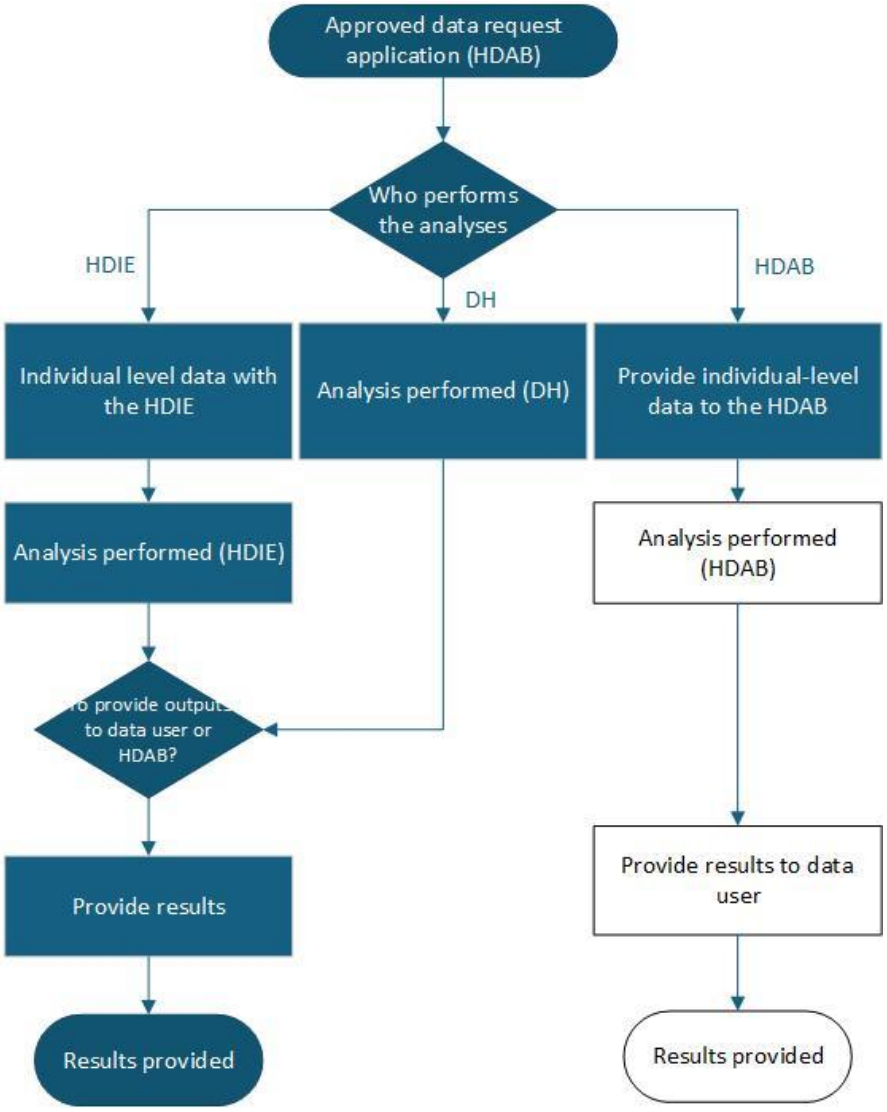


Figure 6 Illustrative workflows for secondary use of electronic health data in case of an approved data request. This figure provides a high-level conceptual illustration of the EHDS landscape and infrastructure, showing how data flows may differ depending on specific conditions.
DH=Data holder, HDIE=Health Data Intermediate entities, DU=Data User, Diamond=choices, Box=process, Oval=begin and end point.



3.6 Interaction and communication in the national EHDS infrastructure

Health data holders must interact with Health Data Access Bodies (HDABs) at various stages of the secondary use process, in accordance with their obligations under Articles 60, 63 and 77 of the EHDS Regulation. While certain interactions are required under the EHDS Regulation, additional exchanges may be needed to ensure proper coordination and compliance, even if not explicitly mandated. These interactions are essential to enable the secure, transparent, and efficient reuse of electronic health data for secondary purposes, such as research, innovation, policy-making, and public health activities.

Communication and interaction between the data holder and other parties within the EHDS-institutional landscape might be needed at different timepoints during the data user journey. Some derive from required EHDS data holder duties, such as when receiving the approved health data application. Besides these mandatory interactions, experts advise that many other interactions can be foreseen that are not specifically stated in the EHDS. Communication channels should be set up for these recommended interactions as well.

3.6.1 Means of communication

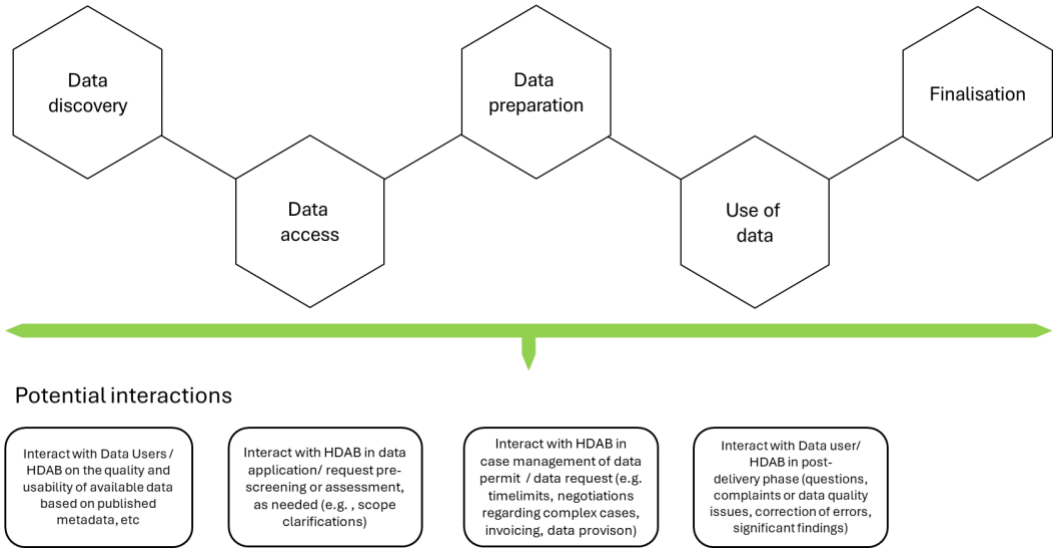
Facilitation of a communication channel between the HDAB and health data holder is recommended, potentially within the SPE or application portal.

Communication between HDABs and health data holders should follow a structured and transparent process to ensure efficiency and accountability. Upon receiving a data access application or data request, the HDAB is responsible for notifying the relevant data holder. In response, the data holder must confirm the feasibility of the request through the corresponding standardised form, which should include the expected timeframe for data delivery as well as an estimate of any justified costs related to data preparation. If the data holder requires additional clarification regarding the data access application or data request, they should initiate contact with the HDAB. See TEHDAS2 M6.3 Guideline for Health Data Access Bodies on the procedures and formats for data access for more details on HDAB responsibilities. Furthermore, email or another mutually agreed communication channel should be used for any correspondence that falls outside the scope of standardised forms, such as informal queries, coordination issues, or follow-up discussions. It is advised that communications hold traceable records to ensure proper documentation and transparency, but also to secure just appeal process' if need be. This requirement aligns with the duty of data holders to provide dataset descriptions (metadata) under Article 60(3) and the duty of HDABs to maintain national dataset catalogues under Article 77(1) EHDS Regulation.

3.6.2 When to communicate and interact

During all phases of the data user journey, where the data holder is involved, interaction will be needed. Figure 7 presents the interactions currently identified during the EHDS User Journey. For more details on the EHDS User Journey, see Annex 6.4. EHDS Data User Journey.

Figure 7 Potential data holder interactions during the User Journey



Cooperation with assessment on data quality and usability

Under Article 60(3) of the EHDS Regulation, data holders are required to ensure appropriate data quality when making data available for secondary use, and under Article 77(2) they must also maintain accurate and up-to-date metadata in their dataset descriptions. In line with these provisions HDABs may, at any time, request further information or clarification from data holders concerning the quality, provenance, or technical characteristics of the electronic health data. Such interactions are part of the HDAB's mandate to ensure that data made available for secondary use meets required standards for integrity and reliability. In response to these requests, data holders are expected to provide timely, complete, and accurate information. This cooperation is essential to the utility of health data made available within the EHDS framework.

Non-compliance

In accordance with Article 63(7), HDABs may take enforcement actions, including warnings, periodic penalties, or temporary restrictions on access, in cases of non-compliance by health data holders.

If a data holder fails to meet its obligations under the EHDS regulation, such as withholding electronic health data, delays in providing data, neglecting to be transparent, or not providing the required metadata, the Health Data Access Body (HDAB) may take corrective or enforcement actions.

A detailed explanation of the fees and penalties can be found in TEHDAS2 M4.1.2 Guideline on penalties for non-compliance related to the EHDS regulation.

3.6.3 Possible data holder interactions

The TEHDAS2 experts have identified topic of potential interactions. This section presents a structured overview of the core interaction points between health data holders and HDABs.

Data format or scope clarification

In circumstances where the scope or structure of a requested electronic health data does not align with the data held, the health data holder must engage with the HDAB to clarify these discrepancies. Such engagement ensures that any inconsistencies are addressed, and that realistic expectations about data availability and formatting are established. If feasible, the data holder should propose alternative formats or data structures that are compatible with the original request. Any adaptations to the data requested should be agreed with the HDAB and may result in updates to the permit conditions (see Art. 68(4) and 70(3)).

Completeness of provided data

The EHDS Regulation does not explicitly mention completeness or quality checks of the provided data. In article 57, it is stated that HDABs must receive, prepare, combine, and anonymise/pseudonymise data (Art. 57, 68), and then make it available in a secure environment (Art. 73). The responsibility for dataset quality sits with the data holder (who may apply a data quality and utility label – Article 78) and the HDAB (who may audit/revoke it – Article 57(1)(d)). These duties imply a quality or completeness check. If the data is deemed complete and sufficient, the HDAB will inform the data user that the data is available. If data is incomplete or incorrect, a request for clarifications and changes to datasets or outputs can be issued by the HDAB. Requests for change can regard technical issues, metadata, or data issues. In this step, interaction is needed to clarify the change or addition needed.

Notification of intellectual property and/or trade secrets

As described in section 3.3.4, health data holders must proactively inform the HDAB if any electronic health data submitted, either during its initial registration or following the issuance of a data permit contains information that is protected by intellectual property rights, trade secrets, or regulatory confidentiality obligations, in accordance with Article 52(2). Upon such notification, appropriate safeguards must be requested to ensure lawful protection of the sensitive elements.

Audits of quality and utility labels

If concerns arise regarding the accuracy of a dataset's quality or utility label, or if the dataset is randomly selected for review, the HDAB may initiate an audit under Article 78(4). During such audits, the data holder must submit all relevant documentation and evidence to substantiate the dataset's assigned labels. Should the submitted evidence be deemed insufficient, the HDAB may revoke the label to preserve the integrity of data quality standards. These audits support the integrity of the EHDS metadata catalogue and are based on the legal mandate of Article 78(4).

Significant Findings

In case of significant findings, the data user will communicate to the HDAB. The HDAB will subsequently inform the health data holder (Art. 58 (3) of the EHDS regulation). The health data holder may shall, under the conditions laid down by national law, inform the natural person or health professional treating the natural person concerned. Natural persons have the right to request not to be informed of such findings. More information regarding significant findings can be found in TEHDAS M8.2 Guideline for Health Data Access Bodies on implementing the obligation of notifying the natural person on a significant finding from the secondary use of health data.

National level interactions

In addition to the obligations set at the EU level, Member States may implement stricter measures and additional safeguards under Article 51(4). Health data holders must therefore ensure compliance with any such national provisions, which may require additional approvals or impose further restrictions on data access and use. Moreover, there may be interactions related to errors that have been found by data users in the provided health data or related to enriched datasets.

Data Analyses

Although not prescribed by the EHDS regulation, good practice shows that to enable the HDAB or data users to perform the correct analyses, they must have a good understanding of the data that is provided so that the correct data analysis can be performed. When data is analysed, questions might be raised to gain clarity for data cleaning, data manipulation and statistical analysis processes.

4 Making data available (Workflow Overview)

The data provision process begins once a data permit or data request approval has been formally issued by a HDAB. Upon issuing a data permit or approving a data request, the HDAB shall immediately request data extraction from the respective health data holder(s) as per Article 60 and Article 68(7) if not otherwise agreed with the health data user.

From that point forward, the health data holder is responsible for:

- Checking which data should be provided according to the data permit or data request approval. (described in section 4.1)
- Preparing the corresponding electronic health data (described in section 4.2),
- Providing the data securely (Chapter 5) to
    - In case of a data permit: the HDAB or a Secure Processing Environment (SPE), or
    - In case of a data request: the anonymised statistical outputs to the data user, HDAB or SPE in accordance with the applicable legal and technical conditions, for further processing by the HDAB

The data provision process concludes when the data or derived results have been successfully delivered to the designated SPE, or when the health data holder has completed the required processing under HDAB supervision. Throughout the process, clear communication with the HDAB and other stakeholders is essential to clarify technical details, timelines, or to resolve uncertainties in the data specification.

The following subsections outline how this provision process functions within the broader EHDS architecture and explain which types of data may be requested, and under what conditions.

FAIR Data

Improving the quality and utility of datasets through informed customer choice and harmonising related requirements at Union level, while applying established standards such as the FAIR principles, brings benefits not only for health data holders, health professionals and natural persons, but also for the Union economy as a whole (EHDS regulation Rec. 85). Article 92 in Chapter VI (European governance and coordination) of the EHDS empowers the European Commission to adopt implementing acts (secondary legislation) to set concrete technical standards and specifications for EHDS. The article explicitly names FAIR principles as a guiding requirement.

The FAIR principles can inexplicitly be found throughout the EHDS regulation, including but not limited to the following articles and their associated implementing acts:

- **Findable**: e.g. addressed via the dataset catalogues (Art. 77).

- **Accessible**: e.g. addressed through transparent procedures and SPEs (Art. 73).
- **Interoperable**: e.g. addressed via common formats, semantic and technical standards (mainly in Chapter 2 (primary use) and 3 (EHR systems and wellness applications)).
- **Reusable**: e.g. addressed through the quality and utility labels and consistent documentation (Art. 78).

For health data holders, TEHDAS2 experts recommend that health data holders follow the FAIR principles to prepare for the EHDS. Please note that FAIR principles are not mandated, but are considered good practice whenever data flows, catalogues, or infrastructures are concerned.

4.1 Which data should be provided

Article 60(1) of the EHDS prescribes that Health data holders shall make relevant electronic health data referred to in Article 51 available upon request to the health data access body, in accordance with a data permit issued pursuant to Article 68. In this section, we describe in short what information the data holder will be provided with by the HDAB when it issues a data permit or a data request approval, and the different steps of the workflow to confirm which data should be provided and how, for each of these application types.

For more details on the HDAB duties for handling health data access applications and health data requests, issuing data permits and coordinating the exchange of electronic health data, read TEHDAS2 M6.3 Guideline for Health Data Access Bodies on the procedures and formats for data access. Additionally, a template of the data access application and data request is presented in the Annexes of the M6.3 guideline.

4.1.1 Data permit

A data permit grants the data applicant permission to process specified anonymised or pseudonymised electronic health data.

The HDAB will send the data permit decision to the data holder together with a specification containing more detailed information of the data to be provided, and a deadline for when the data are to be delivered to the HDAB.

The data permit will provide information needed for the data holder to prepare the required data, including the following:

- In section 6.4 of the permit “Data to be disclosed on the basis of the data permit”, the data holder should be listed together with information on data sources and categories, as well as a short description of the data granted.
- In the same section, information can be found regarding whether the data are to be disclosed to the data user in an anonymised or pseudonymised format.

- Section 6.5 “Data to be disclosed on the basis of the data permit” together with corresponding parts of the specification (Appendix 1) is important to the data holder for understanding how data should be prepared and disclosed.
- Appendix 1 presents a detailed description of the data. The format of the specification may vary between Member States and/or HDABs.

4.1.2 Data request approval

A data request approval grants access for the data applicant to non-personal data in an anonymised statistical format for the purposes referred to in Article 53 of the EHDS regulation (Art. 69(1)). After approval, the HDAB will send the data request approval to the data holder, together with a specification of the required electronic health data, including scope, format, and intended use.

In order to derive anonymised, aggregated statistical outputs from personal or non-personal electronic health data, processing might be required by the data holder (or the intermediation entity carrying out the data holder´s duties) and/or the HDAB.

In such cases where the data holder processes the data, one or more tabulation plans could be provided with the data request approval from the HDAB. Tabulation plans are vital to the data holder when preparing data in a statistical format as they have information on the data user’s needs regarding how the data extraction and compilation of the statistics should be carried out. This includes information on data source(s), variables from each data source to be used, potential new variables to be constructed, the order of creating the statistics, and other factors that are of relevance when producing the requested statistics. (See section 4.2)

Depending on the details of the data request, the health data holder may need to provide individual-level personal data for the HDAB to do further processing to achieve the statistical format to be made available to the data user. This could be the case for example when the HDAB needs to combine data from two or more data holders to produce the requested statistics, or when the HDAB needs to perform or control the exclusion of individuals who have opted out.

4.1.3 Verification

Article 60 of the EHDS regulation states that health data holders shall put the requested electronic health data at the disposal of the health data access body within a reasonable time. Although not specified in the EHDS text, the TEHDAS2 experts recommend the data holder to verify the aspects of the HDAB´s request described below (illustrative examples provided). Some examples of situations in which the data holder might not be able to provide the data in accordance with the request from the HDAB are given. There might be other such situations not described here.

Scope: is it clear which data should be provided and how?

Examples:

- It is not clear whether data should be provided in an anonymised or pseudonymised format
- The described method of selecting a population is unclear, contradictory or mutually exclusive
- Tabulation plans needed for data preparation are not included

Feasibility: is it practically possible to do the data extraction, preparation and provision in the way described?

Examples:

- The population cannot be created using the specified method and/or variables listed in the data permit
- The data is not structured in the way described by the HDAB
- The described data provision to the HDAB would result in files that are too large for transferring to the selected SPE

Timeframe: can it be done and delivered within the requested timeframe?

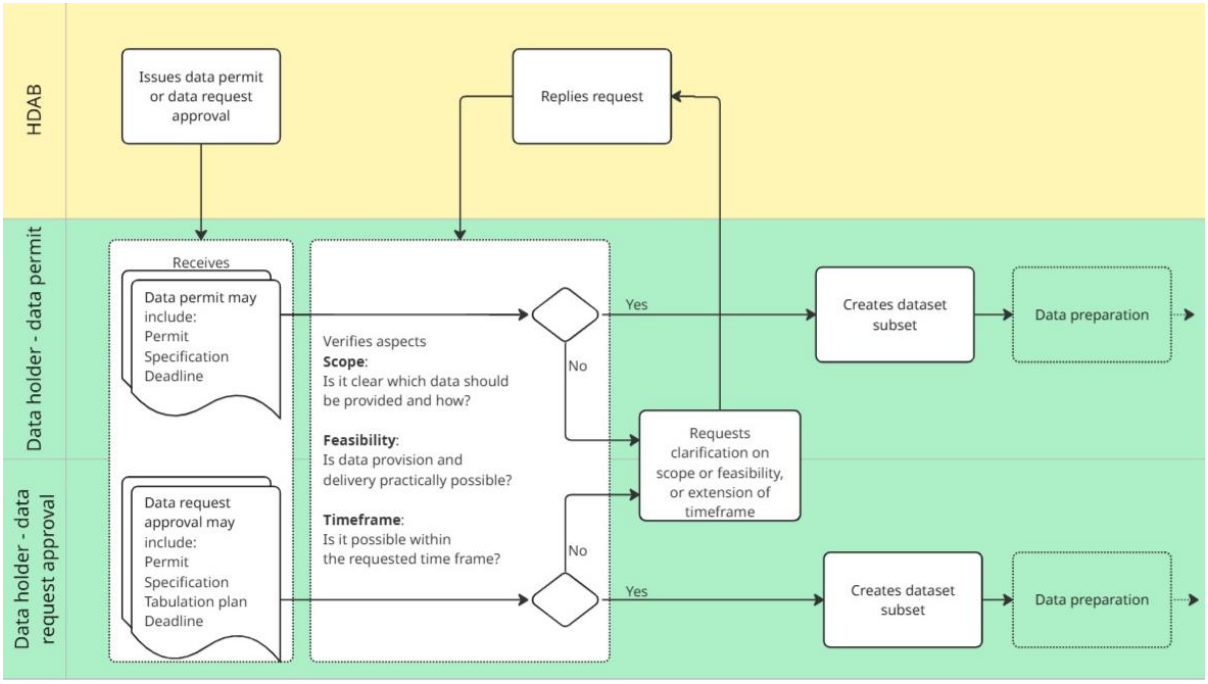
Example:

- The data extraction, preparation or provision has a high level of complexity that cannot be completed within the time frame

We recommend that data holders are involved during the application assessment process. This will give the data holder the opportunity to see and comment the suggested data extraction description and prevent delays later in the process. However, experience shows that clarifications or extra information may be needed from the HDAB or data user after a permit has been issued or data request approved. After receiving a reply from the HDAB with clarifications or information on a potential extension of the timeframe, it is recommended that the data holder verify these aspects again in light of the new information.

Figure 8 provides an Illustrative flowchart of the recommended process of data verification and electronic health data subset creation.

Figure 8. Illustrative flowchart of the recommended process of data verification and electronic health data subset creation by a data holder after receiving a data permit or data request approval from a HDAB. After data preparation, the data provision phase commences.



4.1.4 Data subset creation

The HDAB is responsible for processing electronic health data referred to in Article 51 such as the receiving, combination, preparation and compiling of necessary requested data from health data holders, the pseudonymisation or anonymisation of the data (Art. 57(1)(b)). However, good practice is to perform these activities as close as possible to the source of the data. Therefore, these activities may be performed by the data holder. Data holders that are unable or disinclined to perform these activities, can lay these responsibilities with the HDAB.

The process that the data holder performs with the data before the they are prepared for provision, besides data minimisation, anonymisation, pseudonymisation, management of opt-outs and IP and trade secrets management, is called **data consolidation**. Data consolidation may include creation of a data subsets, data extraction, duplicate elimination, data quality control and data linkage including linkage quality assessment.

In general, a data holder may be requested to provide:

a dataset as described in the dataset catalogue;

- a portion of the data in the catalogued dataset needing a **data extraction** process,

- or to perform combination of data contained in the datasets that the data holder controls (data linkage), often needing **data extraction** from these various datasets

In Annex 4 Considerations for implementation, experience-based recommendations can be found.

4.2 Data preparation

Data preparation refers to the process of transforming and organising electronic health data to comply with a data permit or data request. The HDAB is responsible for processing electronic health data such as the combination, preparation and compiling of necessary requested data from health data holders, and the pseudonymisation or anonymisation of the data (Art. 57(1)(b)). However, good practice is to perform these activities as close as possible to the source of the data. Therefore, this process may be carried out by the health data holder, the HDAB, or another authorised entity (e.g. health data intermediation entity), depending on the arrangement and technical capacity. The HDAB may assume preparation tasks, particularly when the data holder lacks the required technical capacity, or when multiple datasets must be combined or anonymised centrally.

Experts identify the following key steps of data preparation, which will be described in the paragraphs that follow, including:

- Opt-out management;
- Intellectual property and trade secrets and other protected rights management;
- Data minimisation and purpose limitation;
- Pseudonymisation or anonymisation;
- Data linkage;
- Statistical aggregation in case of a data request;
- Data validation before delivery.

It is important to note that the sequence for performing these steps is not set, as a data holder can choose any sequence it judges to be the best, based on the type of data to be processed, on the characteristics of the data permit or data request, or based on its ordinary data processing procedures.

The following table (Table 1) summarises which steps are legal obligations, which are considered good practices, and which coordination points with the HDAB or national choices should be considered.

Table 1. Summary of key steps for data preparation.
HDH=health data holder, HDAB= Health Data Access Body

Step	Responsibilities and obligations	Responsibility of	Relevant EHDS articles	Actions to be carried out
Opt-out management	The EHDS Regulation allows Member States to assign the task of removing opt-outs to either the HDAB or the health data holder. This responsibility should be clearly defined in national law.		71	Remove individuals who opted out
Intellectual property and trade secrets management	Mandatory, only if the HDAB has approved measures that need to be taken by the data holder during data preparation	HDAB, data holder	52	Apply restrictive or technological protection measures
Data minimisation and purpose limitation	Mandatory, responsibility lies with the HDAB. However, process might be delegated to the data holder (optional)	HDAB	66	Trim data to the minimum scope defined in the permit/request
Pseudonymisation or anonymisation	Mandatory, responsibility lies with the HDAB. However, process might be delegated to the data holder (optional).	HDAB	57, 60, 68	Apply pseudonymisation or anonymisation techniques
Data linkage	Combination of datasets by different data holders is the responsibility of the HDAB. Linkage of internal datasets is optional. This is not explicitly required by EHDS text, but it can be necessary if approved by the HDAB. Can also be performed by the HDAB.	HDAB	57	Carry out data linkage of datasets
Statistical aggregation in case of a data request	Mandatory, responsibility lies with the HDAB. However, process might be delegated to the data holder (optional).	HDAB	69	Carry out statistical aggregation of data
Data validation before delivery	Mandatory, the data holder must check whether the data prepared corresponds to the data permit or data request. This process is not explicitly mentioned by EHDS text.	Data holder	60	Carry out data validation checks

The flowchart reported in Figure 9 provides an illustrative example of the process of data preparation by a data holder following approval of a data permit or a data request in the case the HDAB will do the data analysis, whereas the flowchart reported in Figure 10 describes the process of data preparation by a data holder following approval of a data request in the case the data holder will do the analysis. These flowcharts are based on experience from the TEHDAS2 experts. The actual

distribution of preparation tasks depends on the permit/request specification and national implementation.

Figure 9. Illustrative example of the process of data preparation by a data holder following approval of a data permit or of a data request in the case the HDAB will do the analysis. IP=intellectual property.

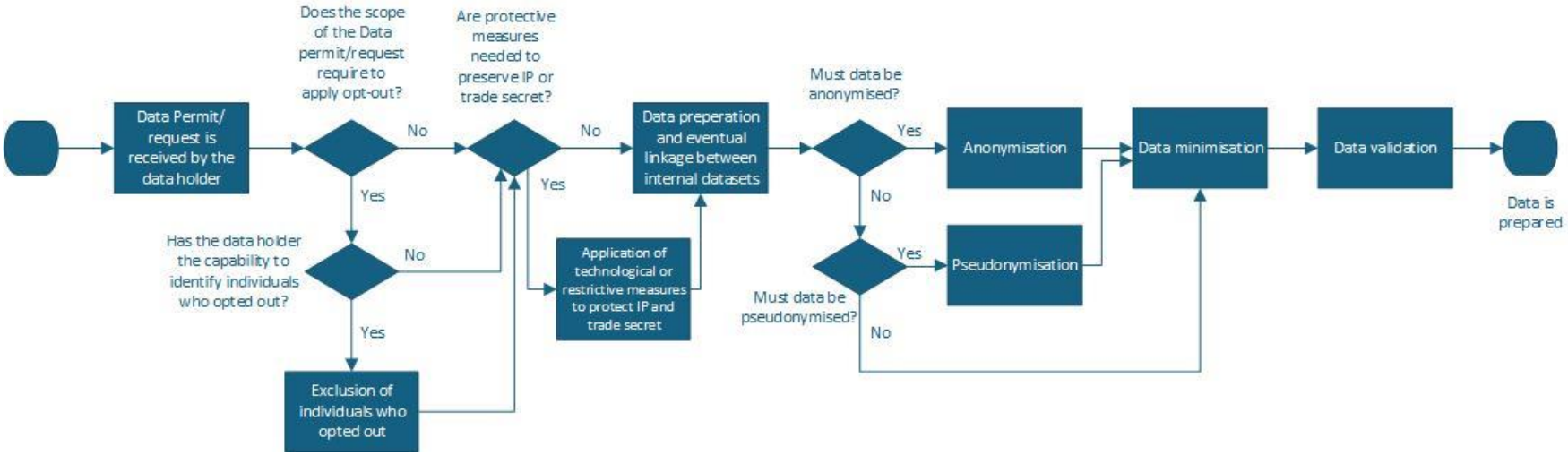
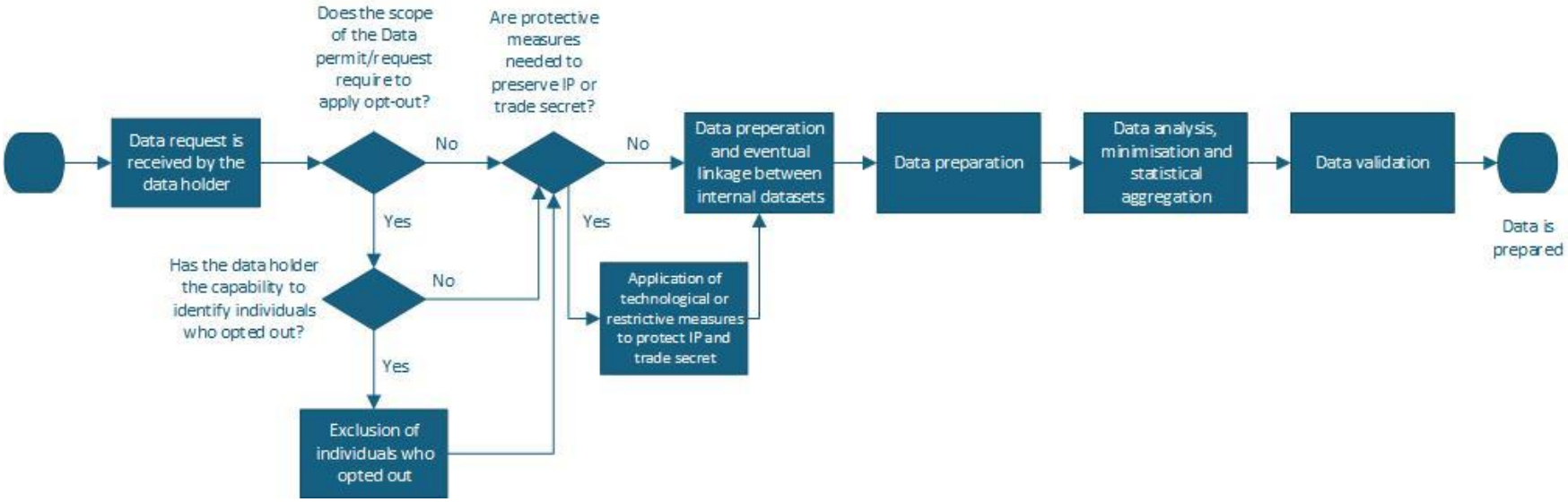


Figure 10. Process of data preparation by a data holder following approval of a data request in the case the data holder will do the analysis. IP=intellectual property



See Checklists for EHDS Health data holders on data preparation in Annex 5.

Opt-out management

The EHDS regulation grants natural persons the right to opt out of the secondary use of their personal electronic health data (Art. 71 (1)). It allows Member States to assign the task of removing opt-outs to either the HDAB, the health data holder or trusted data holder. This responsibility should be clearly defined in national law. Another possibility is that the responsibility is assigned to a Trusted Third Party (TTP).

Operationally, if the responsibility has been designated to the data holder by national laws, it has to strip out the data of persons who have opted out during the data preparation phase, if two preconditions are met (see Figures 9 and 10):

- The scope of the data processing requires to apply the opt-out right i.e. no justified exemptions according to national law were approved by the HDAB (Art. 71(4)).
- The data holder has the capability to link the natural persons who have opted out to the data subjects in the electronic health data. Otherwise, it is recommended that the data holder will only have to notify the HDAB about the lack of ability to make this link.

Further details about the features of the opt-out mechanism and how it may be implemented by Member States can be found in M8.1 “Guideline for Health Data Access Bodies on implementing opt-out from the secondary use of health data”.

Intellectual Property and trade secrets management

Article 52(2) of the EHDS regulation states that health data holders shall inform the HDAB of any electronic health data containing content or information protected by intellectual property rights or trade secrets. At the data preparation stage, it is assumed that the appropriate protection measures have been established by the HDAB according to article 57(1)(c). During data preparation, the data holder of data concerning IP, is recommended to pay particular attention to the implementation of protection measures of technological or restrictive nature, if requested by the HDAB (see Figures 9 and 10). More information on intellectual property and trade secrets can be found in TEHDAS2 M5.1.1 “Guideline for data holders on data description” describing the data holders’ duties regarding data description on Data discovery” and M6.3 “Guideline for Health Data Access Bodies on the procedures and formats for data access”.

Data minimisation and purpose limitation

Article 66(1) describes the responsibility of the HDAB, stating that access is only provided to electronic health data that are adequate, relevant and limited to what is necessary in relation to the purpose of processing indicated in the health data access application by the health data user and in line with the data permit issued pursuant to Article 68.

Although this responsibility is placed with the HDAB, the data holder should also apply data minimisation and purpose limitation principles, as mandated by the GDPR Regulation (Art.

5), to ensure not more data is extracted and provided than necessary from the approved data permit or data request approval.

Data minimisation and purpose limitation measures must be put in place both in the case of a data permit and a data request, and apply to both personal and non-personal data. As stated by articles 68 and 69 of the EHDS Regulation, the HDAB defines the scope of data to be provided during the data application handling phase. A data holder is recommended to ensure a good communication with HDAB, to identify all direct identifiers (e.g., names, ID numbers) or indirect identifiers (e.g., age, ethnicity, education) amongst the requested variables. That enables HDAB to define how to provide these sensitive data: it will identify the transformation that has to be applied to indirect identifiers and the direct identifiers which are to be excluded by the final set of data made available to data user.

Every data application must clearly report the exact selection criteria that data holder has to apply during data preparation, explicitly defining which population, time period and geographic area of interest and which variables are to be provided. See TEHDAS2 M7.2 “Guideline on data minimisation, pseudonymisation, anonymisation and synthetic data” for further information.

Some of the data minimisation tasks can be performed at the beginning of the data preparation phase, whereas others can be performed only after the completion of other operations (e.g. after pseudonymisation or data linkage). In all cases, the data holder must verify that, at the end of the data preparation process, data minimisation and purpose limitations principles are respected, considering that further minimisation may also be done by the HDAB during the subsequent phase of data provision.

Pseudonymisation and anonymisation

Under the EHDS regulation (Art. 66(2)), electronic health data shall be provided in an anonymised format by default, if the purpose of data processing can be achieved with such data, based on the information provided by the data user. Conversely, if the data user has sufficiently justified that the purpose of data processing cannot be achieved with anonymised data (for example, because of the need to identify repeated measurements over time from the same individuals), electronic health data shall be provided in a pseudonymised format (Art. 66(3), Art. 67(2-e)).

Although article 57(1)(b) of the EHDS regulation lays the responsibility of pseudonymisation or anonymisation with the HDAB, it is considered good practice that pseudonymisation and anonymisations occurs as early as possible during the process of making health data available for secondary use and as close as possible at the source. Therefore, these duties will often be delegated to the data holder when able.

Where the data holder is instructed by the HDAB to provide identifiable information, data holders are recommended to separate direct personal identifiers and health records and communicate to HDAB how to link the data. Where the data holder is instructed by the HDAB to conduct pseudonymisation, the data holder should provide pseudonymised data, but only if this allows the HDAB to perform record linkage or exclude individuals who opted out (e.g. if common pseudonymised codes are used at the national level).

The process of pseudonymisation or anonymisation must be governed by clear procedural and technical guidelines. More detailed information can be found in TEHDAS2 M7.2 “Guideline on data minimisation, pseudonymisation, anonymisation and synthetic data”.

Data linkage

Data linkage, the process of combining, joining or merging data from several sources, can be done with respect to the same individuals, or to the same values of any data variable, such as geographical areas or healthcare facilities. Although article 57(1)(b) of the EHDS regulation lays the responsibility of combining the data with the HDAB, data linkage might also be necessary for the data holder, especially when several datasets from one entity (organisation, enterprise) need to be linked.

A detailed description of data linkage procedures can be found in TEHDAS2 M7.5 “Guideline for Health Data Access Bodies on linkage of health datasets”.

Statistical aggregation in case of data requests

In case of a health data request, article 57(1)(b) and 69(1) of the EHDS regulation lay the responsibility of generating an anonymised statistical format with the HDAB. Article 72(6) allows trusted data holders to do the aggregation instead. It is considered good practice that anonymisations occurs as early as possible during the process of making health data available for secondary use and as close as possible to the source. Therefore, these duties might also be delegated to the data holder when able. Capability and capacity will be needed to do the statistical data analysis. If not available, the individual-level data should be provided to the HDAB or intermediation entity to perform the analysis.

A data request approval that is sent to the data holder will contain clear methodological definitions of how the statistical aggregation is to be made. This information will be found in the tabulation plan. M6.3 Guideline for Health Data Access Bodies on the procedures and formats for data access provides more details on the data request and associated data request form and assessment.

Data validation before delivery

Before delivery, the EHDS regulation (Art. 60(1) prescribes a data holder to provide the data for which a data permit or data request approval is issued. This text implies that a data holder should perform a data check to ensure the accuracy of the data with respect to the issued data access permit or data request.

TEHDAS2 experts recommend that this check includes at least the following verifications:

- the absence of missing values where fields are expected to be filled;
- the absence of duplicate rows (with respect to the statistical unit defined in the issued data permit or data request approval);
- completeness of data with respect to the issued data permit or data request approval;

- data type for all columns matches the data specification (e.g., dates are stored as dates, text as text);
- Field names match the data specification;
- Encoded values (e.g., sex = 1 or 2) have explanations;
- The data provided respects the scope and conditions of the data requested by HDAB.

Additional validation steps, such as the identification of outliers, internal consistency checks, or plausibility reviews, are not mandatory under the EHDS Regulation. However, they may be considered good practice by data holders to facilitate data usability and reliability. Any such checks should be performed voluntarily and transparently communicated to the HDAB or data user, where appropriate.

It would constitute a good practice for a data holder to make the HDAB or data user aware of potential data anomalies, such as issues related to:

- missing values,
- inconsistent distributions (e.g., age outside the expected range),
- atypical data patterns (e.g., variable “education level” reporting 95% of values “no qualification” on a population aged 18-65 years),
- coherence (e.g., start date before end date).

Data preparation by trusted data holders

Besides the above-mentioned data preparation processes, trusted data holders may, depending on national arrangements and Article 66(2), take on broader roles in data preparation. Examples of optional processes would be data processing that may need access to external data such as data linkage or information on individuals who opted out.

Time limits for data preparation

The data preparation phase by the data holder must be carried out in reasonable time, to comply with the specific restrictions set within the EHDS regulation. The data holder must provide the requested personal electronic health data to the HDAB no later than three months from receiving the request. In justified cases, this period may be extended by up to three additional months. These time limits for data preparation also apply in case of a simplified procedure for access to electronic health data from a trusted health data holder or accelerated procedure for public sector bodies Figure 4 presents the overall EHDS timelines.

5 Providing Data

Data provision is the process in which an organisation (in this case the data holder) provides personal or non-personal data to the designated recipient under the EHDS Regulation — typically a Health Data Access Body (HDAB) via a Secure Processing Environment (SPE)

In article 60, the EHDS regulation mandates that health data holders shall make relevant electronic health data referred to in Article 51 available upon request to the health data access body, in accordance with a data permit issued pursuant to Article 68, or upon a health data request approved pursuant to Article 69.

In case of a data permit, when the data is prepared, the data holder will provide the data to the HDAB (Art. 68(7)), typically via the SPE operated by the HDAB. When a Member State has designated/authorised one or more external SPE's the data may also be directly provided to such a secure environment (art. 73(2)).

This Chapter describes the potential data flows when providing data. The presented paths are examples of how a member state can organise the data provision and the steps data holders can take during the data provision. They give an indication of processes needed for making health data available based on best practices.

The workflows during the data provision depends on several factors:

- the type of application (data permits and data request approval) i.e. the legal basis for the request,
- the nature of data (personal or non-personal data), and
- the involvement of member state assigned roles such as the trusted data holder or the intermediation entity.

As a data holder, these variables will influence the path to take when providing your data whether through the HDAB's own SPE or a designated external SPE. For cross-border data provision the data will first be provided to the Member State coordinating HDAB, following the same provision process.

5.1 Types of Applications

The procedures for complying with the obligation set out in Article 60 of the EHDS Regulation — i.e. making the relevant electronic health data available via the appropriate channels — may vary depending on Member State infrastructure.

This section presents indicative workflows for the two types of applications defined in the Regulation:

- data permit under Article 68 (individual-level data); and
- health data request under Article 69 (resulting in aggregated outputs).

In case of a data permit, the EHDS article 73 states that that individual-level data is granted through an SPE. In practice, the SPE can be part of the HDAB, part of a Trusted Data Holder, or be an independent organisation.

In case of an approved data request, two may be followed:

- In most cases, the HDAB processes the requested data directly in an SPE without granting access to the individual-level electronic health data to the applicant. The data holder's role is limited to preparing and transmitting the required data to the HDAB.
- In some cases, the data holder may directly process the data to generate the anonymised, aggregated response and provide it to the HDAB, which then delivers it to the data user. The resulting dataset is then transmitted to the HDAB, which remains responsible for providing it to the data user.

Below, possible data flows for each of these options are described in more detail. The presented flows are based on good practice examples.

5.2 Data Permits

Under Article 66, the EHDS Regulation requires that Health Data Access Bodies (HDABs) only make data available to the extent necessary for the approved purpose and, where appropriate, in anonymised or pseudonymised form

It is considered good practice for anonymisation or pseudonymisation, where applicable, to be performed as close to the source as possible — for example, by the data holder before transmitting data to the HDAB or SPE. Therefore, we recommend that in case of a data permit already anonymised or pseudonymised individual-level patient data are provided to the HDAB or selected SPE. To deliver the data to the HDAB, we recommend taking the following steps (also see Figure 11 Flowchart Data for an illustrative example of data provision in case of a data permit):

1) **Contact between data holder and HDAB or SPE:**
   a. Once the data permit is issued, the data holder coordinates with the HDAB or designated SPE to organise the data transmission in accordance with the permit.
   b. During the contact, the following information could be communicated
      - Format of the data
      - Metadata to be added
      - Dataset identifier
      - The location of the HDAB SPE or selected external SPE
      - Means of data transfer
      - The assigned SPE must meet the technical and legal conditions under Articles 73 and 74. The data holder may consult the HDAB to confirm the appropriate safeguards are in place.

2) **Metadata attachment**: When providing data to the HDAB or SPE, good practice is to include metadata to the dataset, including at least the following information:
    a. Dataset Identifier
    b. Versioning
3) **Data encryption**: Recital 4 of the EHDS regulation prescribes that "the sensitivity of personal electronic health data and the sufficient safeguards at both Union and national level needed to ensure a high degree of data protection, security, confidentiality and ethical use". To ensure safe and secure data provision, good practice is to encrypt the data before transferring the data to the designated environment and to share the encryption key separate from the dataset.
   More details on data encryption can be found in TEHDAS2 M7.2 Technical specification for Health Data Access Bodies on data minimisation and de-identification.

4) **Data transmission**: As the EHDS mandates that data is provided safely and securely, we recommend that the data transferral ensues via a secure channel, using the EHDS infrastructure. Examples of data transferral transactions are:
    a. Automatic transferral, for example by a
        – Pull (a pull strategy involves pulling data from a system by the target system)
        – Push (a push strategy involves a source system sending data to a target system)
        – Notified pull (a pull strategy pulling data from the source system after the source system has sent a notification that the data is ready)
    b. Manual transferral, for example by a
        – Drop (a transaction where the data holder copies their data and drops their data into the designated folder in the SPE)

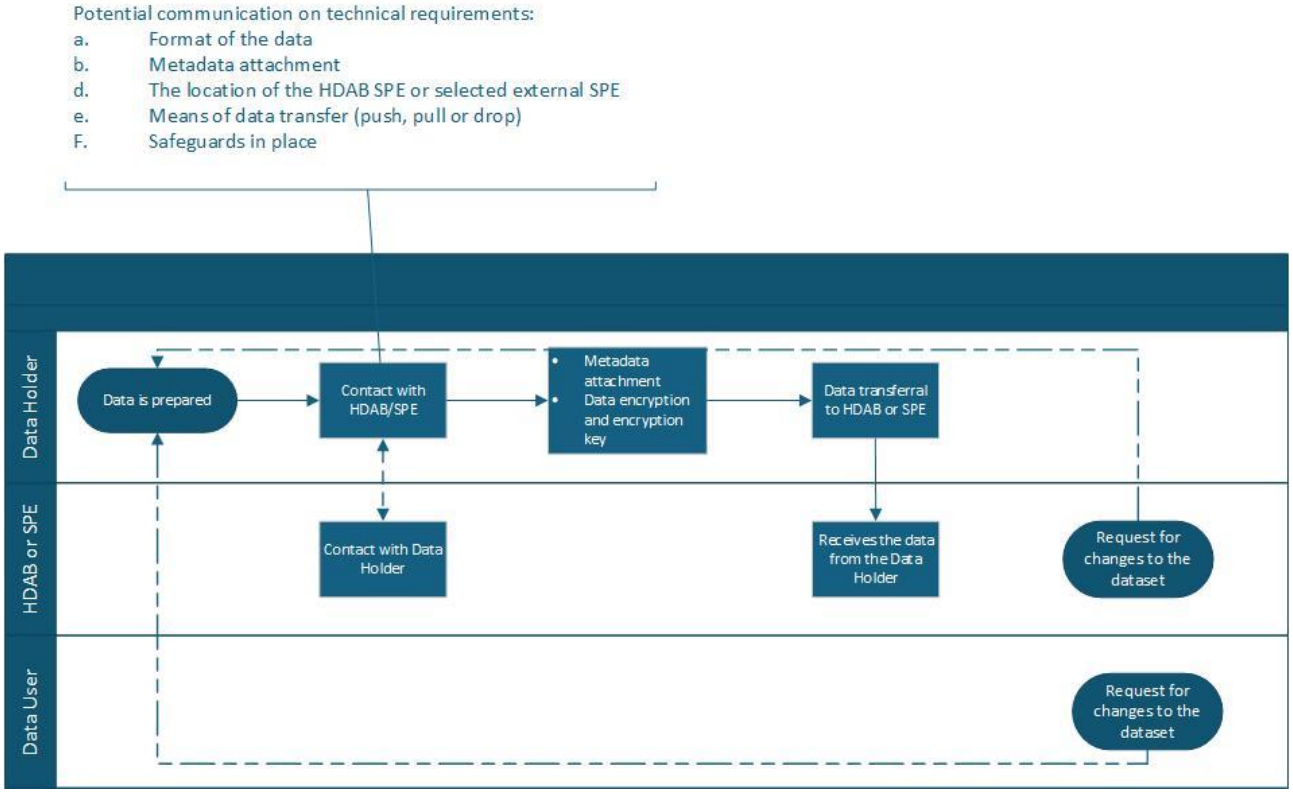
The HDAB may check whether the data received complies with the technical specification and is sufficient to carry out the statistical processing. While the EHDS Regulation does not explicitly require the HDAB to verify data completeness or quality, Articles 57 and 78 outline responsibilities related to preparation and labelling. The HDAB may notify the data holder if data appears incomplete or inconsistent with the permit.

During this step, interaction is needed to clarify the change or addition needed. In case of a request for changes (modifications to the datasets) after data provision, the data holder would be referred back to the data preparation phase. After these changes have been made, the data holder will follow steps 1-4 of the data provision cycle again.

In some cases, the data user may request clarifications or raise concerns through the HDAB. It is considered good practice for HDABs to relay such requests to the data holder where appropriate, particularly in relation to data quality or interpretation.

Data users are consumers of the label — they rely on it when selecting and interpreting datasets. It is considered good practice that data users can issue a request for changes as well after the data is provided. Especially when data quality is lacking, a request for clarifications or changes (modifications to the dataset) might be submitted.

Figure 11 Illustrative example of the flow during data provision in case of data permits.



5.3 Data requests

In case of a data request, as described before, two potential data provision flows can be required:

1) The individual health data is provided to the **HDAB, who will perform the analyses**. The HDAB then provides these results to the data user.
2) The **data holder performs the data analyses** and provides the results to the HDAB or directly to the data user.

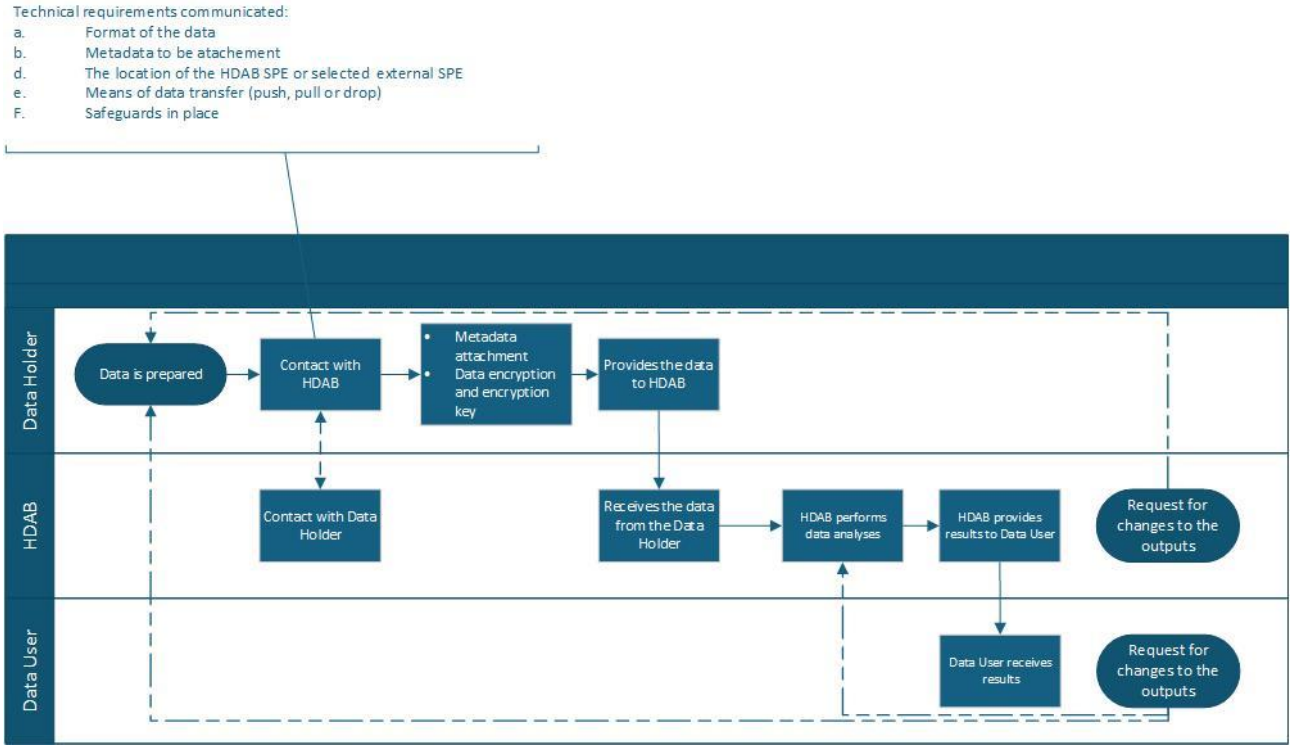
The EHDS Regulation does not prescribe who should perform the statistical aggregation. Depending on the request's complexity and the capacity of the data holder, the aggregation may be carried out by the data holder, a trusted data holder, a Health Data Intermediation Entity, or the HDAB. Cross-border requests or complex linkages may require centralised processing by the HDAB.

A data request can only result in an anonymised statistical output (it is in fact non-personal data). The EHDS Regulation defines "non-personal electronic health data" as data falling outside the scope of the GDPR (Art. 2(2)).

In case of **option 1; the HDAB performs the data analysis,** data provision is similar to the data permit (section 5.1.2). The data holder prepares the data and provides them to the

HDAB, where analysis is performed. Figure 12 presents an illustrative example of the flow in case of a data request when the HDAB does the analysis.

Figure 12 Illustrative example of the flow during data provision in case of data requests, when the HDAB performs the analyses.



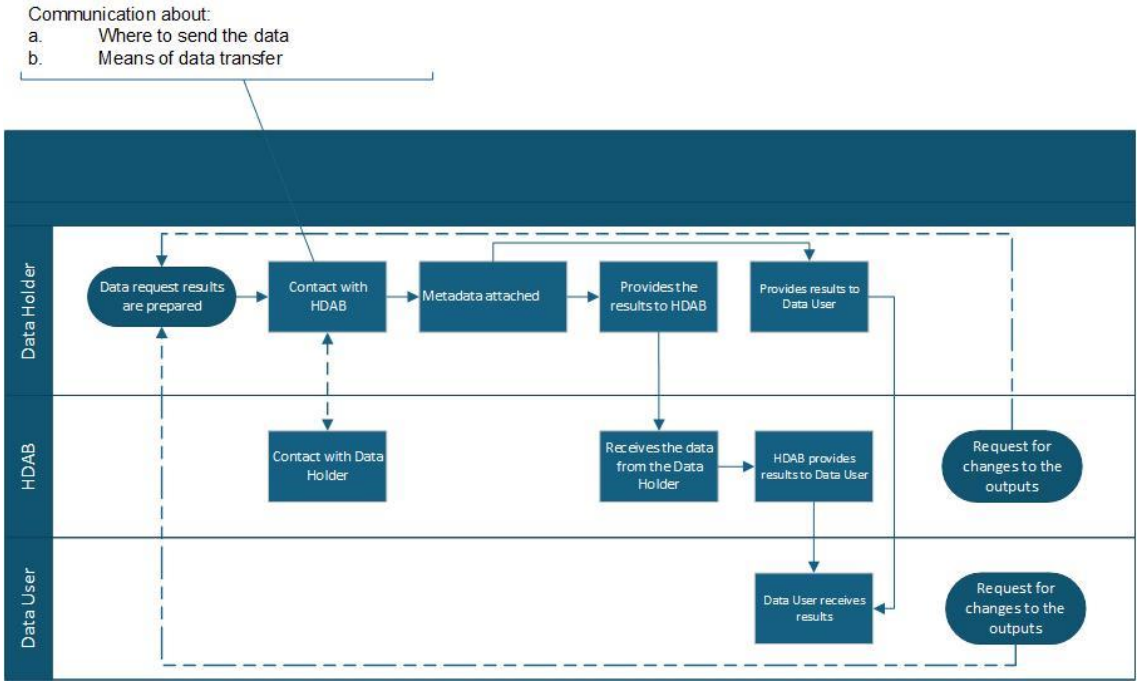
In case of **option 2: the data analyses are performed by the data holder**, only the anonymised statistical output (results of the analyses) would be provided to the HDAB. In case of a trusted data holder, the results could be provided directly to the data user. As the results will be anonymous (in aggregated form), the data provision cycle will be simpler than for the option in which the individual-level data is provided and the HDAB will perform the analysis. The following steps can be taken (Figure 13 Illustrative example of the flow in case of a data request when the (trusted) data holder performs the analysis):

1) **Contact between data holder and HDAB or data user:** The data holder contacts the HDAB or directly the selected SPE that the data is prepared. The following information would at the minimum be communicated
    a. Where to send the data to
    b. Means of data transfer
2) **Metadata attachment**: When providing data to the HDAB or SPE, good practice is to include metadata to the dataset, including at least the following information:
    a. Versioning

3) **Data transferral** to HDAB or Data User. Recommended is to use existing structures for data transferral. As anonymised data falls outside the scope of the GDPR (Art. 2(2)), less privacy restrictions are needed when transferring.

The data user or HDAB may check the results of the data analysis and in case of questions, possibly requiring interaction with the health data holder.

Figure 13 Illustrative example of the flow during data provision in case of data requests, when the health data holder performs the analyses.



5.4 Non-personal data

The EHDS Regulation defines "non-personal electronic health data" as data falling outside the scope of the GDPR (Art. 2(2)). It does not, however, prescribe the precise flows or technical modalities for provision of non-personal data. These are determined at implementation level. The recommendations given in these sections are based on expert opinion of the TEHDAS2 experts.

Depending on whether non-personal data is openly available or subject to restrictions, different provision mechanisms may apply. The following subsections distinguish between:

1. open non-personal health data,
2. restricted non-personal data provided via the HDAB, and
3. linkage scenarios involving both types.

Open data databases

Data holders with non-personal electronic health data publicly available should make this data findable in the dataset catalogue (Art. 60(5)). This statement includes open data databases. However, data holders of open databases do not have an obligation according to the EHDS to provide the data to the HDAB. Data users do not have to get approval by the HDAB to receive the data, and can download these open data independently from the original resource. Recommended is to include the link to the database environment where data should be available for download in the dataset catalogue.

Examples of open data databases can be found in the European data portal (EDP).[6] The EDP holds overs 7,000 datasets related to health, ranging from air pollution, ambulance usage, smoking and accidents. For example, in relation to air pollution the EDP has air quality report from different air stations in Abbatucci, France, maps that show the interpolated air quality within Belgium and reports on CO2 pollutant analysis in cities such as Lecce in Italy. The datasets are provided by national open data portals that collect data from national institutions, such as federal, regional and local portals; national, regional and local government bodies or research institutions.

Access-restricted non-personal data

Some non-personal data will be **access-restricted**. Data such as patient safety data per healthcare organisation or synthetic might be restricted for IP or sensitivity reasons and will not be published in an open data database. However, the EHDS-regulation (art. 60(5)) prescribes the data holders to make their data available for data users when requested and approved by the HDAB.

To provide non-personal, restricted access data, the data provision flow will be similar to the flow in case of personal data. The TEHDAS2 experts recommend including at least the following steps in the data provision:

1. **Contact between data holder and HDAB or SPE.**
2. **Metadata attachment,**
3. **Data encryption**
4. **Data transferral**

For more details per step, please read section 5.1.2 Data Permits

The HDAB or data user may check the data provided. In case of requests for changes by the HDAB or data user, the data holder is referred back to the data preparation phase (section

[6] Data.europa.eu; The official portal for European data. European Union). data.europa.eu.

4.2). After the changes to the data have been made, the data holder will follow steps 1-5 of the data provision cycle again.

This flow is similar to the flow in case of a data permit. Therefore, a visual representation of these steps can be found in Figure 11.

Linkage with open data databases

In case **the open data should be linked** to requested individual patient data, the open data should be provided to the HDAB or the SPE. For example, if a researcher wants to assess the correlation between air pollution and type of lung cancer, they can request lung cancer patient data from a cancer registry and link air pollution data to the lung cancer patients via their post code.

In case of linkage of non-personal data in an open data database to personal data, 2 options may ensue

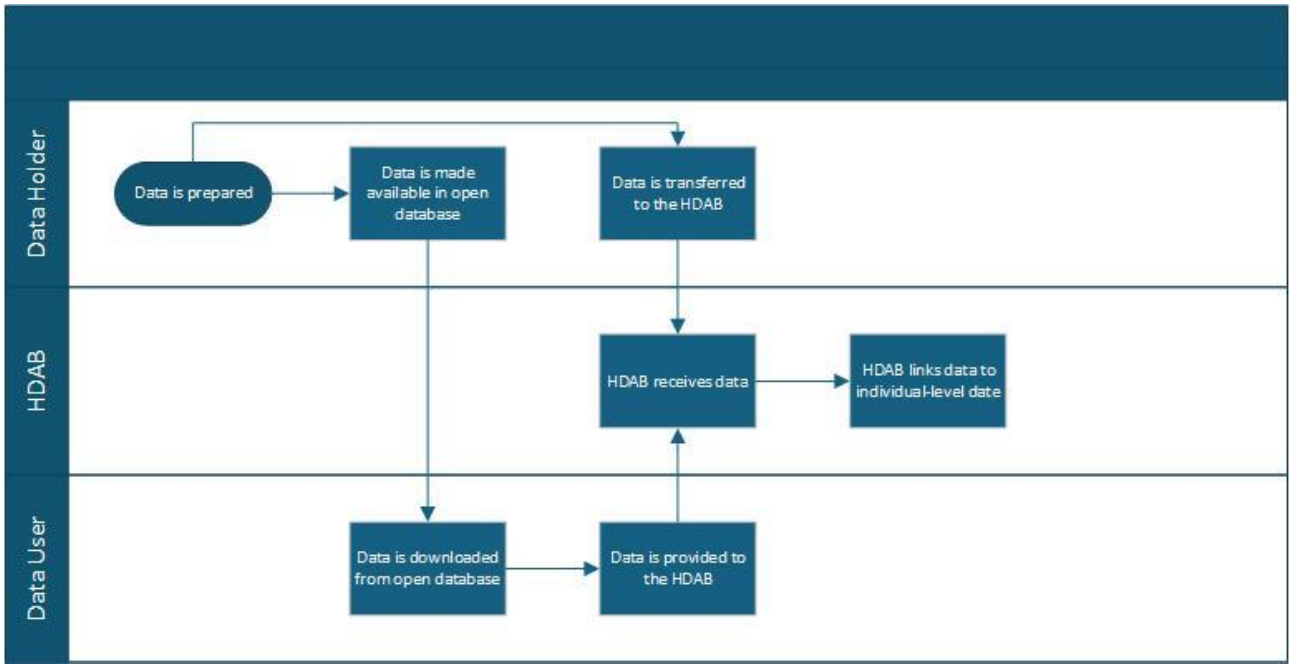
1. The data user will download the relevant open data and provide these to the HDAB or SPE
2. The data holder will provide the non-personal data to the HDAB or SPE.

As the data holder of open databases are only mandated by the EHDS to describe their dataset in the dataset catalogue and ensure findability, the default situation will be that the data user will download the data and provide to the HDAB or SPE (option 1).

If open data is downloaded and combined by the data user, this occurs within the SPE, under HDAB supervision (per Articles 73–74). The HDAB remains responsible for compliance with data protection and security requirements.

Figure 14 describes the possible steps in the data provision process when data between personal and open data are linked.

Figure 14 Illustrative example of the flow during linkage of personal with non-personal data from an open data database



5.5 After the data preparation and provision process

After the data has been prepared and provided, the data use phase commences. During this phase, experts advise that interactions between Data holder and HDAB or data user are foreseen. Possible topics can be:

- **Significant findings**

  In case of significant findings, the data user will communicate to the HDAB. The HDAB will subsequently inform the health data holder (Art 58 (3) of the EHDS regulation). The health data holder may, under the conditions laid down by national law, inform the natural person or health professional treating the natural person concerned. Natural persons shall have the right to request not to be informed of such findings. More details on this topic can be found in M8.3 Guidelines for Secondary Data Users on Handling Research Outcomes, which provides guidance on regulatory, ethical and legal considerations.

- **Questions regarding data or results provided**

  Although not prescribed by the EHDS regulation, the TEHDAS2 experts advise that communication might be needed about data or results provided. When data is analysed by the data user, questions might be raised to gain clarity for data cleaning, data manipulation and statistical analysis processes. Additionally, to indicate their meaning, expertise from the data holder might be needed.

For example, if a data holder has requested data on hospital readmissions from multiple data holders, the numbers might be vastly different. This can be caused by a difference in the definition of an admission, where one hospital includes and other hospitals exclude daycare admissions.

- **Invoicing and additional costs**

  In accordance with the EHDS regulation (Art. 62(2)), if the preparation, formatting, or secure transmission of data involves justified additional costs, the data holder may issue an invoice to the data user, via the HDAB, to recover those expenses. Such costs must be reasonable, transparent, and clearly communicated in advance as part of the feasibility confirmation process. The cost estimate should be included in the standardised response form and must align with the scope of the data access request.

  The process related to fees and invoicing is further described in the TEHDAS2 M4.1.1 'Guideline on fees related to the EHDS regulation' and M4.1.2 'Guideline on penalties for non-compliance related to the EHDS regulation'.

6 What to watch for Nationally

Member States are obliged to ensure that legal, organisational, operational, semantic, technical, safety and cybersecurity measures are in place. The implementation will require several important choices affecting your place as a data holder within the EHDS legal and technical architecture. As a data holder, in preparation for the EHDS you need to be aware of the progress and choices made in the Member State in which the data is included in the national metadata catalogue (Art. 60(3), Art. 77(1)).

Based on emerging implementation discussions, at least four configurations of the EHDS-infrastructure may arise, based on the position of the coordinating HDAB and the National Contact Point (NCP).

1. Member States with one single HDAB with the role of Coordinator HDAB operating the HDAB Coordinator Portal and the NCP
2. Member States with several distinct HDABs, and one HDAB with both role of Coordinator HDAB and NCP operator.
3. Member States with one single HDAB with the role of Coordinator HDAB and another legally designated organisation operating as NCP.
4. Member States with several distinct HDABs, one Coordinator HDAB and another legally designated organisation operating NCP.

Regarding secondary use, by 26 March 2029, their HDABs must be ready to receive applications, as well as be connected to HealthData@EU. By 26 March 2031, the HDABs must be ready to also exercise their tasks regarding the final categories of data (Art. 51).

The EHDS regulation text is not yet specific on many topics. The EHDS regulation will be supplemented by a number of Delegated Acts. Informative and non-binding documents such as the TEHDAS2 guidelines and the EC "Frequently Asked Questions on the European Health Data Space" [7] will support data holders in their understanding of the EHDS.

However, many choices that remain will be tackled by Member States. Besides the pattern of the infrastructure, these choices will have implications for the data holders regarding their interactions and paths to walk in data preparation, provision and interactions with the other EHDS roles.

Examples of choices made by Member States that will influence the data holders' duties, responsibilities, and processes:

- Governance and the national authority responsible for EHDS implementation:
  - Designation of coordinating HDAB and NCP
  - One or multiple HDABs assigned
  - To assess expertise required and ensure appropriate personnel is in place
  - Potential extension of duties regarding micro-enterprises
  - Decisions on fees that can be charged
  - Potential additional categories of electronic health data
- Technical infrastructure and interoperability standards:
  - Implementation of services such as a national dataset catalogue and the DAAMS.
  - Assigning trusted data holders and intermediation entities
  - Designating national SPE(s) used for the EHDS infrastructure (can also be assigned locally or regionally)
- Rules for accessing electronic health data, ensuring security and privacy.
  - Setting up the national opt-out system (including responsibilities)
  - Providing in its national law for a mechanism to make data for which a right to opt out has been exercised available (under strict conditions)
  - Choose exceptions for which opt-out is not required
  - Deciding on where to lay the responsibility of data security and privacy measures such as anonymisation and pseudonymisation (also dependent on Member State organisation maturity)
  - Data access procedures: Establish clear and transparent procedures for authorising and granting data access, including ethical and privacy considerations
- Aligning EHDS implementation with existing national health data systems:
  - Define technical infrastructure, interoperability standards, and requirements for national data-sharing frameworks.
  - Specify national standards to ensure data usability and reliability.

[7] Frequently Asked Questions on the European Health Data Space , European Commission 4dd47ec2-71dd-49fc-b036-ad7c14f6ed68_en

To prepare as a data holder, it is essential that you follow your Member State progress, and the choices made on these topics.

7 Considerations for data holders – discussion

The health data holders across Europe have a key role laying the foundation for health data use and reuse, for the potential benefit to individuals and society. The EHDS regulation marks a significant initiative to make European health data more findable, accessible and useful for the intended secondary purposes. However, the realisation of this goal depends largely on the efforts of Member States and the data holders, including assessment of their own ability and capacity not only to fulfil the mandated duties in EHDS but also their broader commitment to foster data quality, to ensure effective data management and to participate in communication with other stakeholders.

- In Chapter 3, the legal duties of health data holders under the EHDS Regulation are described. Beyond these obligations, the guideline stresses the need for internal systems, secure data transfers, and effective communication to enable secondary use of health data under the EHDS directive.
- Chapter 4 outlines how health data holders must make data available once a permit or request has been approved, including identifying which data to provide, preparing it according to requirements, and transferring it securely via a designated SPE. Beyond these obligations, the guideline highlights good practices such as verifying feasibility, applying anonymisation or pseudonymisation close to the source, performing data validation, and using tabulation plans to support accurate and efficient provision of data for secondary use.
- Chapter 5 describes the process of providing data once it has been prepared, including delivering personal data via an SPE for data permits and supplying anonymised statistical outputs for data requests in line with the EHDS Regulation. Beyond these obligations, the guideline points to good practices assuring secure data transmission and responding to requests for clarifications and requests for changes.

While there is a set of defined duties and tasks for data holders to comply with, it is evident that this draft guideline cannot go beyond the basic common elements of the requirements in relation to the preparation and provision of any health data for secondary use. Detailed guidance for data holders on how to proceed with initial assessment or what to consider in preparation would depend on multiple factors, including understanding of the individual business processes and needs in the different types of organisations and settings. Any natural or legal person as well as organisation that qualifies as health data holder according to the EHDS criteria will need to assess - in their specific context - their own ability and capacity to fulfil these duties. Dimensions to consider in relation to a data holder’s ability and capacity concern the level of maturity and/or expertise regarding e.g. data collection, data

management and governance, infrastructure, data access procedures from a legal, ethical and technical perspective (See Annex 3 Maturity levels).

To fully prepare for implementation of EHDS as a data holder there are several other topics to explore further.

The joint work performed in TEHDAS2 and other European initiatives (please see Annex 6 Data holder resources for more references), and the feedback from stakeholders through several public consultations will help to develop a shared understanding of what data holders may need guidance on for the implementation of EHDS. There are opportunities for Member States to develop tailored context-relevant guidance as well as promote sharing of knowledge and best practices across stakeholders.

.

Annex 1 TEHDAS2 Glossary

Key terminology in our guideline

Term	Definition
Anonymisation	The process by which personal data is altered in such a way that a data subject can no longer be identified directly or indirectly. (Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, Recital 52; EHDS Regulation, Recital 92)
Data controller	A data controller is a person or organisation that determines the purposes and essential means of the processing of personal data. The role of the data controller can be shared by several people or organisations. In that case, they are defined as joint controllers. The controller is accountable and responsible for establishing a lawful data processing workflow and observing the rights of data subjects. (GDPR Article 4(1)(7)).
Data extraction	Data extraction is the process of retrieving data from its source dataset. Structured data extraction involves extracting data from datasets that are already organised in predefined formats. Unstructured data extraction pertains to extracting data from databases handling unstructured formats such as PDFs, images, or free text. There may be one or more different data sources from which data extraction may be required.
Data linkage	The process of combining ***datasets*** ”from several sources on one topic or data subject” (ISO 5127:2017, 3.1.11.12). This can be done using unique identifiers, probabilistic methods, or a combination of techniques.

Data minimisation	A principle mandating organisations to only collect, store and process the minimum necessary amount of personal data for a specific purpose. This principle is fundamental under GDPR and relevant to the tasks outlined in EHDS. (GDPR Article 5(1)(c)). Access is only provided to electronic health data that is "adequate, relevant and limited to what is necessary in relation to the purpose of processing indicated in the health data access application by the health data user and in line with the data permit issues pursuant to Article 68." (EHDS Regulation, Article 66(1)) Data minimisation applies to all stages of the data lifecycle
Data permit	An administrative decision issued to a health data user by a Health Data Access Body to process certain electronic health data specified in the data permit for specific secondary use purposes based on conditions laid down in Chapter IV of the EHDS regulation (Art. 2(2v)).
Data preparation	Data preparation is the process in which an organisation (in this case the data holder) transforms and organises raw personal or non-personal health data into one or more datasets (either in individual-based or aggregated form), to comply with a data permit or a data request approval issued by a Data User and approved by the competent Health Data Access Body.
Data Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. (GDPR Article 4(2))
Data Provision	The stage in the data user journey where prepared health data is made accessible to authorised users for secondary purposes.
Data quality	Data quality means the degree to which the elements of electronic health data are suitable for their intended primary use and secondary use; (EHDS Article 2 (2)(z))

Data quality and utility label	Data quality and utility label means a graphic diagram, including a scale, describing the data quality and conditions of use of a dataset. (EHDS Article 2 (2)(aa))
Dataset	A structured collection of electronic health data. (EHDS Article 2(2)(w))
Dataset Catalogue	A collection of dataset descriptions, arranged in a systematic manner and including a user-oriented public part, in which information concerning individual dataset parameters is accessible by electronic means through an online portal. (EHDS Article 2(2)(y))
Data Subset creation	Dataset subset contains only selected records, variables or elements from a larger dataset while maintaining its key characteristics and relationships. Data subset creation refers to the process of extracting the specific portion of a larger database based on defined criteria, in order to support a particular analysis or creation of a statistical format. This evolves extraction of relevant observation and variables for the specified purpose.
Electronic health data	Personal or non-personal electronic health data (EHDS Article 2(2c)).
Health data access application	An application seeking to access personal-level electronic health data for secondary use in an anonymised or a pseudonymised format (EHDS Article 67).

Health Data Access Body	Member State-designated authority that facilitates the secondary use of electronic health data. HDABs assess the information provided by the health data applicant and decide on health data requests and access applications, authorise and issue data permits, obtain data from data holders and make data available in Secure Processing Environments. HDABs systematically track the data request and data access applications received and the data permits issued. As per Article 58 of the EHDS regulation, HDABs are required to publicly list information on the data permits issued. (EHDS Article 55 and Recital 52) The HDAB duties include: • Publishing the data dataset catalogue; • Evaluating health data access applications; • Maintaining records on data access applications and decisions; • Inform citizens on the use of data, the conditions under which data are made available and on how their rights are protected and safeguarded, respectively; • Receiving, preparing and compiling the requested datasets when requested, and properly anonymising or pseudonymising them; • Preserving the confidentiality of intellectual property rights and trade secrets; • providing access to electronic health data to health data users pursuant to a data permit in an SPE; • Supervising and enforcing the compliance of data holders and data users; • If a Member State has provided for the right to opt out pursuant to Article 71 to be exercised through the (coordinating) health data access bodies, the relevant health data access bodies shall provide public information about the procedure to opt out and facilitate the exercise of that right.
Health data applicant	A natural or legal person submitting a health data access application or a data request to a Health Data Access Body for the purposes referred to in Article 53 of EHDS.

Health data holder	Any person, organisation or public body involved in healthcare, care services, health-related products, wellness apps or health(care) research, that has the right to process data for health care provision or for public health purposes, reimbursement, research, policy making, official statistics or patient safety. This includes, for example, hospitals, insurers, research institutes and EU institutions. For a more detailed definition: EHDS regulation, Article 2(2)(t)) .
Health Data Intermediation Entities (HDIE)	A legal person that may be established by national law for the purpose of fulfilling the obligations of certain categories of health data holders and that is able to process, make available, register, provide, restrict access to and exchange electronic health data for secondary use provided by health data holders. (EHDS Regulation, Article 50 (3) and Recital 59)
Health data request	A request to access data in an anonymised statistical format for the purposes referred to in EHDS Article 53. (EHDS Regulation, Article 69)
Health data user	A natural or legal person, including Union institutions, bodies, offices or agencies, which has been granted lawful access to electronic health data for secondary use pursuant to a data permit, a health data request approval or an access approval by an authorised participant in HealthData@EU. (EHDS Article 2(2u)) The rights and responsibilities of heath data users include: ○ Accessing and processing electronic health data exclusively in accordance with an issued data permit, an approved health data request, or access approval from the relevant authorised participant within HealthData@EU. ○ Ensuring that electronic health data processed within secure processing environments is not shared or disclosed to third parties who are not explicitly identified in the data permit. ○ Refraining from re-identifying or attempting to re-identify natural persons from the electronic health data they have obtained, ○ Publicly disseminating results or outputs from secondary use within 18 months following either the completion of electronic health data processing in the secure processing environment or upon receipt of responses to health data requests,

	○ Informing the health data access body of any significant finding related to the health of the natural person whose data are included in the dataset, ○ Cooperating fully with health data access bodies to facilitate the effective performance of their supervisory tasks.
Intellectual Property (IP)	(a) a trade mark; (b) a design; (c) a copyright or any related right as provided for by national or Union law; (d) a geographical indication; (e) a patent as provided for by national or Union law; (f) a supplementary protection certificate for medicinal products as provided for in Regulation (EC) No 469/2009 of the European Parliament and of the Council of 6 May 2009 concerning the supplementary protection certificate for medicinal products (1); (g) a supplementary protection certificate for plant protection products as provided for in Regulation (EC) No 1610/96 of the European Parliament and of the Council of 23 July 1996 concerning the creation of a supplementary protection certificate for plant protection products (2); (h) a Community plant variety right as provided for in Council Regulation (EC) No 2100/94 of 27 July 1994 on Community plant variety rights (3); (i) a plant variety right as provided for by national law; (j) a topography of semiconductor product as provided for by national or Union law; (k) a utility model in so far as it is protected as an intellectual property right by national or Union law; (l) a trade name in so far as it is protected as an exclusive intellectual property right by national or Union law. (Regulation concerning customs enforcement of intellectual property rights and repealing, Article 2(1))
Intermediation entity (IE)	A legal person that may be established by national law for the purpose of fulfilling the obligations of certain categories of health data holders and that is able to process, make available, register, provide, restrict access to and exchange electronic health data for secondary use provided by health data holders. (EHDS reg. Art 50 (3) and Rec. 59)
Invoice	A legally binding commercial document, detailing the complete cost structure with breakdowns by services and data holders. It contains disaggregated cost elements, typically at the task level to favour clarity and transparency.
Non-compliance	Any failure to comply with any requirement under the Union harmonisation legislation or under this Regulation; ((EC) No 765/2008 and (EU) No 305/2011)

Non-personal electronic health data	Electronic health data other than personal electronic health data, including both data that have been anonymised so that they no longer relate to an identified or identifiable natural person (the 'data subject') and data that have never related to a data subject. (EHDS Regulation, Article 2(2b))
Open data	Data in an open format that can be freely used, re-used and shared by anyone for any purpose. 'Open format' means a file format that is platform-independent and made available to the public without any restriction that impedes the re-use of documents; ((EU) 2019/1024 Open Data Directive)
Open (data) database	Publicly accessible digital data that anyone can freely use, reuse, and redistribute for any purpose.
Personal electronic health data	Data concerning health and genetic data, relating to an identified or identifiable natural person, processed in an electronic form. (EHDS Regulation, Article 2(2a))
Pseudonymisation	The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person. (GDPR Article 4(5))
Purpose limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. (GDPR article 5(1b)).
Secondary use	Processing of electronic health data for the purposes set out in Chapter IV of EHDS Regulation, other than the initial purposes for which they were collected or produced. (EHDS regulation, Article 2(2e))
Secure Processing Environment (SPE)	An environment in which access to electronic health data can be provided in following a data permit. An SPE is subject to technical and organisational measures and security and interoperability requirements. Specifically allowing access to only those persons listed in the permit, as well as user authentication, authorisation, restricted data handling, logging and the compliance monitoring of respective security measures. (EHDS regulation, Article 73)

Synthetic data	Data that is artificially generated. The concept of synthetic data generation is to take an original data source (dataset) and create new, artificial data, with similar statistical properties from it.
Tabular data	Data organised in a structured format of rows and columns, where each row represents a single record or entity, and each column represents a specific attribute or variable. This structure is commonly found in spreadsheets or relational databases, making it easy to store, query, and analyse. Tabular data is often used for structured datasets where relationships between variables are well-defined.
Trade secret(s)	Information which meets all of the following requirements: (a) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (b) it has commercial value because it is secret; (c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret. (Trade Secret Directive (2016/943), Article 2(1))
Trusted health data holder	Member State designated health data holder for whom a simplified procedure can be followed for the issuance of data permits. Trusted health data holders leverage their expertise on the data they hold to assist the Health Data Access Body by providing assessments of data requests or access applications. Once data permits are authorised, these trusted data holders provide the data within a Secure Processing Environment that they manage. (EHDS, Article 72 and Recital 76)
Trusted Third Party (TTP)	A pseudonymisation entity that processes identifiers into pseudonyms. (ENISA, Pseudonymisation techniques and best practices, p. 10, modified). The TTP needs only to know only the identifiers of the data subjects on the basis of which it will compute the pseudonyms, and no other data (EDPB Guideline 01/2025, §126).

Annex 2 Links to the EHDS regulation

Relevant EHDS articles (for references)

In the EHDS regulation, health data holder duties for making health data available are included in several articles. Additionally, other articles contain influence data holders and their duties. Relevant articles for this guideline are:

1) Main articles:

Article 51 Minimum categories of electronic data for secondary use - Article 51 'Minimum categories of electronic data for secondary use' states the minimum categories of electronic data for secondary use of which the health data holders have to make the categories of electronic data available. These 17 categories are represented by a diverse set of data holders.

"1. *Health data holders shall make the following categories of electronic health data available for secondary use in accordance with this Chapter:*
(a) electronic health data from EHRs;
(b) data on factors impacting on health, including socio-economic, environmental and behavioural determinants of health;
(c) aggregated data on healthcare needs, resources allocated to healthcare, the provision of and access to healthcare, healthcare expenditure and financing;
(d) data on pathogens that impact human health;
(e) healthcare-related administrative data, including on dispensations, reimbursement claims and reimbursements;
(f) human genetic, epigenomic and genomic data;
(g) other human molecular data such as proteomic, transcriptomic, metabolomic, lipidomic and other omic data; 209/329 EN
(h) personal electronic health data automatically generated through medical devices;
(i) data from wellness applications;
(j) data on professional status, and on the specialisation and institution of health professionals involved in the treatment of a natural person;
(k) data from population-based health data registries such as public health registries;
(l) data from medical registries and mortality registries;
(m) data from clinical trials, clinical studies, clinical investigations and performance studies subject to Regulation (EU) No 536/2014, Regulation (EU) 2024/1938 of the European Parliament and of the Council34 , Regulation (EU) 2017/745 and Regulation (EU) 2017/746;
(n) other health data from medical devices ;
(o) data from registries for medicinal products and medical devices;
(p) data from research cohorts, questionnaires and surveys related to health, after the first publication of the related results;
(q) health data from biobanks and associated databases

2. Member States may provide in their national law that additional categories of electronic health data are to be made available for secondary use pursuant to this Regulation.

3. Member States may establish rules for the processing and use of electronic health data containing improvements related to the processing of those data, such as correction, annotation or enrichment, based on a data permit pursuant to Article 68.
4. Member States may introduce stricter measures and additional safeguards at

national level aimed at safeguarding the sensitivity and value of the data that fall under paragraph 1, points (f), (g), (i) and (q). Member States shall notify the Commission of those measures and safeguards and, without delay, of any subsequent amendment affecting them."

Article 60 Duties of health data holders - Article 60 describes the health data holder duties. This is a main article covered by task 6.1.

1. Health data holders shall make relevant electronic health data referred to in Article 51 available upon request to the health data access body, in accordance with a data permit issued pursuant to Article 68, or upon a health data request approved pursuant to Article 69.
2. Health data holders shall put the requested electronic health data referred to in paragraph 1 at the disposal of the health data access body within a reasonable time and no later than three months from the receipt of the request by the health data access body. In justified cases, the health data access body may extend that period by a maximum of three months.
3. The health data holder shall communicate to the health data access body a description of the dataset it holds in accordance with Article 77. The health data holder shall, at a minimum on an annual basis, check that its dataset description in the national dataset catalogue is accurate and up to date.
4. Where a data quality and utility label accompanies the dataset pursuant to Article 78, the health data holder shall provide sufficient documentation to the health data access body for that body to verify the accuracy of the label.
5. Health data holders of non-personal electronic health data shall ensure access to data through trusted open data bases to ensure unrestricted access for all users and data storage and preservation. Trusted open public databases shall have in place a robust, transparent and sustainable governance and a transparent model of user access.

Article 63 Enforcement by health data access bodies - Article 63 describes the enforcement by health data access bodies towards the health data holder.

1. When carrying out their monitoring and supervisory tasks, as referred to in Article 57(1), point (a)(ii), health data access bodies shall have the right to request and receive all the necessary information from health data users and health data holders to verify compliance with this Chapter.
2. Where health data access bodies find that a health data user or health data holder does not comply with the requirements of this Chapter, they shall immediately notify the health data user or health data holder of those findings and take appropriate measures. The health data access body concerned shall give the health data user or health data holder concerned the opportunity to state their views within a reasonable period that shall not exceed four weeks.
Where the finding of non-compliance concerns a possible breach of Regulation (EU) 2016/679, the health data access body concerned shall immediately inform the supervisory authorities under that Regulation and provide them with all relevant information concerning that finding.
4. With regard to non-compliance by health data holders, where a health data holder withholds the electronic health data from health data access bodies with the manifest intention of obstructing the use of electronic health data, or does not respect the deadlines set out in Article 60(2), the health data access body shall have the power to fine the health data holder for each day of delay with a periodic penalty payment, which shall be transparent and proportionate. The amount of the fines shall be established by the health data access body in accordance with national law. In the event of repeated breaches by the health data holder of the obligation of cooperation with the health data access body, that body may exclude or initiate proceedings to exclude, in accordance with national law, the

health data holder concerned from submitting health data access applications pursuant to this Chapter for a period of up to five years. During the period of that exclusion, the health data holder shall remain obliged to make data accessible under this Chapter, where applicable.
5. The health data access body shall communicate the enforcement measures taken pursuant to paragraphs 3 and 4, and the reasons on which they are based, to the health data user or health data holder concerned, without delay, and shall lay down a reasonable period for the health data user or health data holder to comply with those measures.

Article 68 Data permit - Article 68 covers data permits and the time limits for providing the data.

7. Following the issuance of the data permit, the health data access body shall immediately request the electronic health data from the health data holder. The health data access body shall make available the electronic health data to the health data user within two months of receiving them from the health data holders, unless the health data access body specifies that the data are to be provided within a longer specified timeframe.

Article 69 Health data request - Article 69 covers health data requests.

1. The health data applicant may submit a health data request for the purposes referred to in Article 53 with the aim of obtaining a response only in an anonymised statistical format. A health data access body shall not provide a response to a health data request in any other format and the health data user shall have no access to the electronic health data used to provide that response.
4. The health data access body shall assess the health data request within three months of receipt of the request and, where possible, subsequently provide the response to the health data user within a further three months.

2) Additional articles and topics related to task 6.1:

Article 52 Intellectual property rights and trade secrets - Article 52 describes how to handle intellectual property related to the EHDS data provision.

Intellectual property rights and trade secrets

1. Electronic health data protected by intellectual property rights, trade secrets or covered by the regulatory data protection right laid down in Article 10(1) of Directive 2001/83/EC of the European Parliament and of the Council 35 or Article 14(11) of Regulation (EC) No 726/2004 of the European Parliament and of the Council 36 shall be made available for secondary use in accordance with the rules laid down in this Regulation.

2. Health data holders shall inform the health data access body of any electronic health data containing content or information protected by intellectual property rights, trade secrets or covered by the regulatory data protection right laid down in Article 10(1) of Directive 2001/83/EC or Article 14(11) of Regulation (EC) 726/2004. Health data holders shall identify which parts of the datasets are concerned and justify the need for the specific protection of the data. Health data holders shall provide that information when communicating to the health data access body the description of the dataset they hold pursuant to Article 60(3) of this Regulation or, at the latest, following a request received from the health data access body.

3. Health data access bodies shall take all specific appropriate and proportionate measures, including of a legal, organisational and technical nature, they deem necessary to protect the intellectual property rights, trade secrets or the regulatory data protection right laid down in Article 10(1) of Directive 2001/83/EC or Article 14(11) of Regulation (EC) 726/2004. Health data access bodies shall remain responsible for determining whether such measures are necessary and appropriate.

4. When issuing data permits in accordance with Article 68, health data access bodies may make the access to certain electronic health data conditional on legal, organisational and technical measures, which may include contractual arrangements between health data holders and health data users for the sharing of data containing information or content protected by intellectual property rights or trade secrets. The Commission shall develop and recommend non-binding models of contractual terms for such arrangements.

5. Where the granting of access to electronic health data for secondary use entails a serious risk of infringing intellectual property rights, trade secrets or the regulatory data protection right laid down in Article 10(1) of Directive 2001/83/EC or Article 14(11) of Regulation (EC) No 726/2004 which cannot be addressed in a satisfactory manner, the health data access body shall refuse access to the health data applicant to such data. The health data access body shall inform the health data applicant of, and provide to the health data applicant a justification for, that refusal. Health data holders and health data applicants shall have the right to lodge a complaint in accordance with Article 81 of this Regulation.

Article 57 Tasks of Health Data Access Bodies - Article 57 describes the tasks and duties of the health data access bodies. Some of those tasks relate to the communication with the health data holder.

(a) (iii) requesting electronic health data referred to in Article 51 from relevant health data holders pursuant to a data permit issued or a health data request approved;;
(b) process electronic health data referred to in Article 51 such as the receiving, combination, preparation and compiling of necessary requested data from health data holders, the pseudonymisation or anonymisation of the data;
(c) taking all measures necessary to preserve the confidentiality of intellectual property rights, for regulatory data protection and to preserve the confidentiality of trade secrets as provided for in Article 52, taking into account the relevant rights of both the health data holder and health data user;
(d) cooperate with and supervise data holders to ensure the consistent and accurate implementation of the data quality and utility label set out in Article 56;

Article 58 Obligations of health data access bodies towards natural persons - Article 58 describes obligations of HDABs towards natural persons. However, communication between HDAB and health data holder is included in sub-paragraph 3.

(3) Where a health data access body is informed by a health data user of a significant finding related to the health of a natural person, as referred to in Article 61(5), the health data access body shall inform the health data holder about that finding. The data holder shall, under the conditions laid down by national law, inform the natural person or health professional treating the natural person concerned. Natural persons shall have the right to request not to be informed of such findings.

Article 61 Duties of health data users - Article 61 talks about duties of health data users. However, one sub-paragraph talks about communication towards the health data holder (via the HDAB).

5. Without prejudice to paragraph 2, health data users shall inform the health data access body of any significant finding related to the health of the natural person whose data are included in the dataset.

Article 62 Fees - Article 42 talks about the fees related to a data access or permit request... This article is relevant for task 6.1 because communication is needed between the HDAB and health data holder.

1. Health data access bodies, including the Union health data access service, or trusted health data holders referred to in Article 72 may charge fees for making electronic health data available for secondary use.

The fees shall be in proportion to the cost of making the data available and they shall not restrict competition. The fees shall cover all or part of the costs related to the procedure for assessing a health data access application or a health data request, for issuing, refusing or amending a data permit pursuant to Articles 67 and 68 or for providing a response to a health data request submitted pursuant to Article 69, including costs related to the consolidation, preparation, pseudonymisation, anonymisation and provision of the electronic health data. Member States may establish reduced fees for certain types of health data users located in the Union, such as public sector bodies or Union institutions, bodies, offices and agencies with a legal mandate in the field of public health, university researchers or microenterprises.

2. The fees referred to in paragraph 1 of this Article may include compensation for the costs incurred by the health data holder for compiling and preparing the electronic health data to be made available for secondary use. In such cases, the health data holder shall provide an estimate of such costs to the health data access body. Where the health data holder is a public sector body, Article 6 of Regulation (EU) 2022/868 shall not apply. The part of the fees linked to the health data holder's costs shall be paid to the health data holder.

4. Where health data holders and health data users do not agree on the level of the fees within one month of the data permit being issued, the health data access body may set the fees in proportion to the cost of making electronic health data available for secondary use. Where health data holders or health data users disagree with the fee set by the health data access body, they shall have access to dispute settlement bodies in accordance with Article 10 of Regulation (EU) 2023/2854.

Article 66 Data minimisation and purpose limitation - Article 66 describes the enforcement by health data access bodies towards the health data holder.

Data minimisation and purpose limitation

1. Where health data access bodies receive a health data access application, they shall ensure that access is only provided to electronic health data that are adequate, relevant and limited to what is necessary in relation to the purpose of processing indicated in the health data access application by the health data user and in line with the data permit issued pursuant to Article 68.

2. Health data access bodies shall provide electronic health data in an anonymised format, where the purpose of processing by the health data user can be achieved with such data, taking into account the information provided by the health data user.

3. Where the health data user has sufficiently demonstrated that the purpose of processing cannot be achieved with anonymised data in accordance with Article 68(1), point (c), health data access bodies shall provide access to electronic health data in pseudonymised format. The

information necessary to reverse the pseudonymisation shall be available only to the health data access body or an entity that acts as a trusted third party in accordance with national law.

Article 71 Right to opt-out from the processing of personal electronic health data for secondary use - Article 71 describes the Right to opt-out from the processing of personal electronic health data for secondary use. This article might be relevant in the communication between the HDAB and the health data holder and provision of the data, as an option must exist to provide data of patients that have opted out when relevant.

3. Once natural persons have exercised the right to opt out, and where personal electronic health data relating to them can be identified in a dataset, personal electronic health data relating to those natural persons shall not be made available or otherwise processed pursuant to data permits issued under Article 68 or health data requests under Article 69 approved after the natural person has exercised the right to opt out. The first subparagraph of this paragraph shall not affect the processing for secondary use of personal electronic health data relating to those natural persons pursuant to data permits or health data requests that were issued or approved before the natural persons exercised their right to opt out. .

4. By way of exception from the right to opt out provided for in paragraph 1, a Member State may provide in its national law for a mechanism to make data for which a right to opt out has been exercised available provided that all the following conditions are fulfilled: ...

8. When the purposes of the processing of personal electronic health data by a health data holder do not or no longer require the identification of a data subject by the controller, that health data holder shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with the right to opt out under this Article.

Article 72 Simplified procedure for access to electronic health data from a trusted health data holder - Article 72 describes the Simplified procedure for access to electronic health data from a trusted health data holder.

Simplified procedure for access to electronic health data from a *trusted health* data holder

1. Where a health data access body receives a health data access application pursuant to Article 67 or a health data request pursuant to Article 69 that only covers electronic health data held by a trusted health data holder designated in accordance with paragraph 2 of this Article, the procedure set out in paragraphs 4 to 6 of this Article shall apply.

2. Member States may establish a procedure whereby health data holders can apply to be designated as trusted health data holders, provided the health data holders meet the following conditions:

(a) they are able to provide access to health data through a secure processing environment that complies with Article 73;
(b) they have the necessary expertise to assess health data access applications and health data requests;
(c) they provide the necessary guarantees to ensure compliance with this Regulation.

Member States shall designate trusted health data holders following an assessment of the fulfilment of those conditions by the relevant health data access body. Member States shall establish a procedure to regularly review whether the trusted health data holder continues to fulfil those conditions. Health data access bodies shall indicate the trusted health data holders in the dataset catalogue referred to in Article 77.

3. *Health data access applications and health data requests referred to in paragraph 1 shall be submitted to the health data access body, which may forward them to the relevant trusted health data holder.*

4. Following receipt of a health data access application or health data request pursuant to paragraph 3 of this Article, the trusted health data holder shall assess the health data access application or health data request against the criteria listed in Article 68(1) and (2) or Article 69(2) and (3), as applicable.

5. The trusted health data holder shall submit the assessment it carries out pursuant to paragraph 4, accompanied by a proposal for decision, to the health data access body within two months of receipt of the health data access application or health data request from the health data access body. Within two months of receipt of the assessment, the health data access body shall issue a decision on the health data access application or health data request. The health data access body shall not be bound by the proposal submitted by the trusted health data holder.

6. Following the health data access body's decision to issue the data permit or to approve the health data request, the trusted health data holder shall carry out the tasks referred to in Article 57(1), points (a)(i) and (b).

7. The Union health data access service referred to in Article 56 may designate health data holders that are Union institutions, bodies, offices or agencies which comply with the conditions laid down in paragraph 2, first subparagraph, points (a), (b) and (c), of this Article as trusted health data holders. Where it does so, paragraph 2, third and fourth subparagraphs, and paragraphs 3 to 6 of this Article shall apply mutatis mutandis.

Article 73 Secure processing environment - Article 50 addresses the Secure processing environment (SPE). This is relevant to task 6.1 because this is the location that the data needs to be provided to. As there might be multiple SPEs, the correct location needs to be communicated. Relevant sub-articles are presented here.

2. Health data access bodies shall ensure that electronic health data from health data holders in the format specified in the data permit can be uploaded by those health data holders and can be accessed by the health data user in a secure processing environment. Health data access bodies shall review the electronic health data included in a download request to ensure that health data users are only able to download nonpersonal electronic health data, including electronic health data in an anonymised statistical format, from the secure processing environment.

Article 74 Controllership - Article 74 provides guidance on controllership.

1. The health data holder shall be deemed controller for the making available of personal electronic health data requested pursuant to Article 60(1) to the health data access body. The health data access body shall be deemed controller for the processing of the personal electronic health data when fulfilling its tasks pursuant to this Regulation. Notwithstanding the second subparagraph of this paragraph, the health data access body shall be deemed to act as a processor on behalf of the health data user acting as a controller for the processing of the personal electronic health data pursuant to a data permit issued under Article 68 in the secure processing environment when providing data through such environment or for the processing of such data pursuant to a health data request approved under Article 69 for a response to be generated.

2. In situations referred to in Article 72(6), the trusted health data holder shall be deemed controller for its processing of personal electronic health data related to the provision of electronic health data to the health data user pursuant to a data permit or a health data request. The trusted health data holder shall be deemed to act as a processor on behalf of the health data user when providing data through a secure processing environment.

3. The Commission may, by means of implementing acts, establish a template for agreements between controllers and processors under paragraphs (1) and (2) of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 98(2).

Article 75 HealthData@EU - Article 75 refers to HealthData@EU. It talks about cross-border access to data.

1. Each Member State shall designate one national contact point for secondary use. That national contact point for secondary use shall be an organisational and technical gateway, enabling and responsible for the making available of electronic health data for secondary use in a cross-border context. The national contact point for secondary use may be the coordinator health data access body pursuant to Article 55. Each Member State shall inform the Commission of the name and contact details of the national contact point for secondary use by ... [the date of entry into force of this Regulation + 24 months]. The Commission and the Member States shall make that information publicly available.

2. The Union health data access service shall act as the contact point of the Union's institutions, bodies, offices and agencies for secondary use and shall be responsible for making electronic health data available for secondary use.

Article 78 Data quality and utility label - Article 78 covers the data quality and utility label. When a data request is approved and data is provided, a data quality and utility label can be attached to the data (health by the data holder). When this label might be inaccurate, this must be communicates from the HDAB to the data holder, and the label might have to be revoked.

1. Datasets made available through health data access bodies may have a Union data quality and utility label applied by the health data holders.

2. Datasets with electronic health data collected and processed with the support of Union or national public funding shall have a data quality and utility label covering the elements set out in paragraph 3.
3. The data quality and utility label shall cover the following elements, where applicable: (a) for data documentation: metadata, support documentation, the data dictionary, the format and standards used, the source of the data and, where applicable, the data model; (b) for assessment of technical quality: completeness, uniqueness, accuracy, validity, timeliness and consistency of the data; (c) for data quality management processes: the level of maturity of the data quality management processes, including review and audit processes, and bias examination

Annex 3 Maturity levels

This Annex provides a structured reference to assess the organisational and infrastructural maturity of health data holders and Member States in preparation for the application of Chapter IV of the EHDS regulation, which becomes applicable from March 2029 for most data categories. The maturity guidance herein builds upon criteria developed in EU-funded initiatives, notably the **QUANTUM project**, the (first) **TEHDAS Joint Action**, and preparatory activities supported by the European Commission under the Digital Europe Programme. It reflects policy insights and practical readiness dimensions for secondary use of health data, aligned with Articles 50 to 78 of the EHDS Regulation and informed by practical implementation scenarios and use cases. The information supports the incremental development of national infrastructures, institutional capacities, and data governance systems that comply with the EHDS legal framework, while allowing for differentiated starting points and growth trajectories among Member States and health data holders. The maturity levels should be treated as illustrative examples.

A 3.1 Maturity level at health data holder level

In the national context, health data holders must assess their organisational maturity to determine their readiness to comply with the obligations established by the European Health Data Space (EHDS) Regulation. This assessment should be aligned with structured maturity models, such as those developed by the QUANTUM project, and reflect clear criteria across various levels, from initial or basic to advanced or optimised. A clear articulation of maturity levels helps distinguish between baseline compliance and advanced capabilities. A basic or entry-level maturity implies that a data holder has minimum capabilities to describe datasets (Art. 77), respond to data access requests (Art. 68), and ensure secure data sharing within prescribed timelines (Art. 60(2)). At the highest levels, organisations are able to provide automated data extraction, manage data across multiple domains, implement advanced privacy-preserving techniques (Art. 66), and proactively support data quality and utility labelling (Art. 78).

While both minimally and highly capable and equipped data holders may comply with EHDS requirements, the ability to create meaningful subsets of data or extract specific variables from complex systems such as electronic health records represents a more advanced maturity. For example, two organisations may list "electronic health record data" in a data catalogue, but only one may be technically capable of isolating specific variables such as concrete disease, its stage, therapy, mortality or prescription history in the existing datasets for reuse. Higher capabilities enhance dataset granularity, facilitate reuse, and increase responsiveness to data permits (Art. 68). This should be acknowledged in maturity evaluations and labelling schemes. Advanced capabilities do not negate the compliance of less-equipped data holders but indicate a higher performance tier.

Institutional maturity is also reflected in governance and risk management systems. Mature organisations have internal mechanisms to flag intellectual property or trade secret concerns early in the permit process (Art. 52), reducing processing delays and ensuring legal

compliance. Institutions with robust policies are better positioned to support both primary governance functions and secondary use, including obligations tied to data altruism and public interest research under Articles 53 and 54.

Capacity plays a decisive role. Larger health data holders must ensure that their systems can scale appropriately to manage the increased volume and complexity of processing in line with EHDS requirements. Smaller entities, particularly those with microenterprise status exempted under Article 50 paragraph 1, may in some cases require support to fulfil their obligations efficiently. Depending on the national context and legal provisions, this support might be facilitated through the delegation of responsibilities to health data intermediation entities, as envisaged under Article 50 paragraph 3. This approach allows Member States to accommodate a wide range of organisational capacities and capabilities of various data holders while maintaining coherence with the overall EHDS framework.

Steps toward readiness for beginner health data holders

For health data holders at the beginning of their digital transformation in secondary use of health data, the pathway to EHDS readiness should be achievable through a set of foundational steps. These include:

1. **Definition of tasks and responsibilities** within the organisation/enterprise, allocation of staff and tools and (IT) technologies necessary for making health data available.
2. **Dataset identification and registration**: Clearly identify datasets relevant under Article 51 and ensure their registration with the Health Data Access Body, including submission of dataset descriptions in line with Article 60 paragraph 3 and Article 77.
3. **Timely data provisioning**: Establish procedures to respond to data requests within three months, extendable once, as outlined in Article 60 paragraph 2.
4. **Governance structures**: Define internal responsibilities for data controllership and, where applicable, joint controllership in compliance with Article 60 paragraph 2.
5. **Secure data handling**: Develop basic capabilities for secure data transmission (Art. 60 (5)) and coordinate with the Health Data Access Body for any required pseudonymisation or anonymisation under Article 66.
6. **Personnel training**: Ensure relevant staff are trained on their duties regarding access, opt-out mechanisms (Art. 71), secure processing environments (Art. 73), and interaction with the Health Data Access Body.

These measures, while foundational, constitute the core of what is required to comply with the EHDS Regulation. Importantly, they provide a scalable basis upon which more advanced capabilities can be gradually developed. Beginners that establish sound data governance and cooperative procedures with national structures can meet their obligations effectively without having to implement complex technical systems from the outset.

The QUANTUM maturity model and EHDS guidelines provide a shared reference framework that can support such incremental growth while ensuring alignment with European standards. [8]

A3.2 Maturity level at Member State level

The national context plays a foundational role in enabling health data holders to fulfil their duties. Member States are responsible for setting up the necessary legal, organisational, and technical framework for secondary use, including:

- ***Deployment of Digital Infrastructure***
  Member States must ensure the availability of secure processing environments, national dataset catalogues, and connections to HealthData@EU. The maturity of these infrastructures will define the operational feasibility of data access (Art. 73, 75, 77).

- ***Implementation of National Legal Options***
  Several EHDS provisions allow Member States to define national rules, for example:
  - National design of the opt out mechanism and infrastructure (especially regarding responsibilities)
  - Exceptions to opt-out mechanisms (Art. 71(4)),
  - Stricter safeguards for sensitive data (Art. 51(4)),
  - Delegation of obligations to health data intermediation entities (Art. 50(3)).

  Early clarification and communication of these national choices are critical for coordinated implementation.

- ***Support Measures for health data holders***
  In more mature systems, national authorities may offer:
  - Centralised data services,
  - Harmonised templates,
  - Legal and technical guidance,
  - Capacity-building initiatives.

These frameworks reduce fragmentation and resource demands at the institutional level. The variability in national progress will directly impact how ready individual health data holders can be by 2029.

A minimum set of so-called digital business capabilities can be defined as a prerequisite for a Member State's participation in the EU HealthData@EU platform. These digital business capabilities result from the obligations enshrined in Chapter IV of the EHDS Regulation for the establishment of national HDABs in Member States and include:

[8] QUANTUM Deliverable 1.2 Specification for the assessment of data holders´ maturity

a) data access application management system - to streamline the process of requesting and granting data access;

b) national dataset catalogue of health data - to provide a comprehensive and searchable listing of available health data sets;

c) secure processing environment - to ensure that health data is processed in a secure and compliant manner;

d) cross-border gateway for HealthData@EU - to facilitate the safe and efficient exchange of health data across borders;

e) health data quality enhancement - to improve the accuracy, completeness, and reliability of health data;

f) opt-out management system - mechanism to allow natural persons to opt-out from secondary use;

g) HDAB transparency portal – to make publicly available information related to secondary use of health data (e.g. applications, permits, results).

In 2021/2022 the TEHDAS1 Joint action assessed Member State maturity in 12 European countries. The following domains were covered in the assessment: data sources, data quality, data infrastructure, data storage, data access, data interoperability, data governance, resources and the EHDS. Each showed a wide variety.

1. Develop and structure electronic health data sources
Member States should begin by mapping and organising their health data assets, such as electronic health records, disease registries, survey data, and biobanks. Building a clear and accessible data landscape is essential to enable both national and cross-border data sharing and reuse.

2. Build interoperable and secure data infrastructure
Creating a strong digital infrastructure means using internationally recognised data models and standards, developing dataset catalogues, and enabling secure processing environments. Embracing federated analysis tools, like the Personal Health Train, allows data to be analysed without needing to move it, enhancing both privacy and efficiency.

3. Strengthen legal and governance frameworks
Legal clarity is key. Member States should align their national laws with EHDS requirements, clearly define, opt-out procedures, and ensure secure systems for identity verification and data access. A solid governance structure will help build public trust and streamline data access.

4. Ensure adequate resources
A successful health data system needs the right people, skills, and funding. This includes

training and retaining data stewards, legal and ICT professionals, and ensuring financial support is in place for infrastructure development and ongoing operations.

5. Promote capacity building and training

Healthcare professionals and data users must be equipped with the knowledge and skills to handle health data responsibly. Providing ongoing education on structured data input, data standards, and digital literacy is crucial to maintaining data quality and integrity.

6. Adopt and share best practices

Member States are encouraged to apply proven technologies, such as privacy-preserving tools and federated analysis models, and share their experiences through European networks and initiatives. This collective knowledge helps raise the bar across the continent.

Annex 4 Considerations for implementations

As the EHDS regulation doesn't specify the process of making data available, this guideline provides recommendations according to good practice and expert opinion. During the writing of this guideline on making personal and non-personal data available, questions and considerations arose. TEHDAS2 experts discussed many open questions that derive from the EHDS legal texts and shared good practice examples. Although not in the EHDS regulation text, it could be useful to share these conversations and thoughts. This Annex discussed some of these considerations for implementation.

The Q&A, illustrative examples and elaborations below are intended to illustrate possible approaches and share real-world examples that may assist preparation for the EHDS. This section is structured according to the legal obligations of health data holders under the EHDS regulation and Data preparation phase.

A4.1 Legal obligations of health data holders under the EHDS regulation

The definitions and statements used in the EHDS regulation could be open to different interpretations. During the writing process, questions were raised and discussed regarding health data holder's duties, Electronic Health Data and datasets. Some of the questions that arose during the writing are discussed below.

- *When and to whom does the EHDS regulation apply in relation to the processing of electronic health data?*
  The EHDS Regulation applies when electronic health data, whether personal or non-personal, is processed by a health data holder as defined in Article 2(2)(t).

- *Does the EHDS regulation apply to the processing of data held for purely personal or household activities?*
  This will be dependent on the site of storage of the data and the allocation of the data controller role. If it is only stored locally in the personal device then it is out of scope since the manufacturer or citizen (e.g. in case of a wellness app on the mobile phone) is not a data holder.

- *What is a dataset and what is structured data according to the EHDS regulation?*
  'Dataset' is defined in article 2(2)(w) as meaning a structured collection of electronic health data. Structured data has a predefined format that facilitates processing. The concept of structured data is not a defined legal term but some examples are given for context in recital 56: "records in a relational database, XML documents or CSV files and free text, audios, videos and images provided as computer-readable files"

- *How can the different duties of health data holders be applied or delegated?*
  The EHDS identified multiple roles regarding data processing, including data holders, trusted data holders, and health data intermediation entities. In some categories of data (Art. 51) it can be difficult to draw a clear line between the role of health data

holder, a HDIE, and a trusted health data holder. To support understanding, illustrative examples are provided below to highlight the distinctions between these types of organisations. These illustrative examples are non-binding and serve only as interpretative guidance

- **Data holder** – e.g. a Research Database:
  A research consortium collects and organises primary care data under data-sharing agreements. However, it lacks the technical capacity or legal guarantees to become a trusted data holder or serve as an HDIE. It remains a regular data holder under Article 60.

- **Trusted data holder** – Quality Registry:
  A national or regional registry collects and curates data from hospitals under contractual agreements. It meets all the conditions to be recognised as a trusted data holder and is assessed and designated as such by the HDAB. It performs assessments of health data access applications and health data requests and may provide access directly under EHDS rules.

- **HDIE** – Regional Centre for Secondary Use:
  A public or private organisation is designated by a Member State to support small healthcare providers (e.g. general practices) in preparing and delivering health data for secondary use. The regional centre does not own or control the data but acts as a processor on behalf of the data holders, enabling compliance with technical and procedural requirements under EHDS. The healthcare organisations will have a data processing contract with the regional centre in which the duties that are transferred will be described.

Important Distinction:
Data made available via an HDIE will always go through the normal application process at the HDAB. In other words, the HDIE functions as a data processor for the health data holder. They do not appear in the public dataset catalogue as autonomous entities. Data processed by an HDIE is still attributed to the original health data holder(s).

A4.2 Examples of non-personal data

The EHDS provides duties regarding making non-personal data available. However, the text remains unclear on the definitions and potential infrastructure regarding these types of data. Please note that also in case of non-personal data, only data within the scope of **Article 51** is within scope. To help health data holders understand the types of data that could be non-personal data under the EHDS, listed below are some illustrative examples of non-personal data per category, as referred to in section 3.3.3:

1) *Data which was initially personal data, but has been anonymised and cannot be attributed in any way to a specific person*

Real life examples are:

- Results from Data requests or data analysis in aggregated or anonymised form (statistics)
- Administrative data (e.g. healthcare use statistics). Take note: An administrative heath data register might be person identifiable, while statistics on degree of coverage of hospital beds in an ICU would be anonymous.
- Mortality and morbidity statistics
- Public health databases (vaccination statistics etc)
- Results from feasibility analyses
- National COVID-19 dashboards
- Healthcare expenditure and financing
- Market level sales data by active substance

2) *Data which does not relate to an identified or identifiable natural person*

Some data that was never related to a natural person is considered health data. Often these regard risk factors or are related to public health. The European Commission Frequently Asked Questions on the European Health Data Space states that detailed socioeconomic data collected outside healthcare settings, or purely environmental data not linked to health." is out of scope of the EHDS. However, in practice, these data are often available in open databases and relevant to researchers.

Real life examples are:[9]

- Data on water quality and flooding risk in an environmental atlas
- Meteorological and Climatology data
- Heat-maps in urban areas
- A map of locations of health care facilities
- Measurements of COVID-19 in sewage water
- Social economic status statistics per post code.
- Non-personal data from Post-Market Surveillance process of a medical device

3) *Fully synthetic databases (de novi creation of data based on predefined rules, models or simulations)* [10]

Regarding synthetic data, a public discussion is currently being held about when synthetic data is fully non-personal. Here we provide a few examples of fully synthetic databases, in which the data is not derived from personal data, but is created de novo.

- A one-million longitudinal clinical synthetic database of medical records (Mitre Corporation)
- A synthetic household population database including location and descriptive sociodemographic attributes of households
  A synthetic database including data of 30,000 beneficiaries with claims data

[9] Open health data on the European Data Portal | data.europa.eu

[10] Gonzales A, Guruswamy G, Smith SR (2023) Synthetic data in health care: A narrative review. PLOS Digital Health 2(1): e0000082. https://doi.org/10.1371/journal.pdig.0000082

A4.3 Elaborations on the data preparation phase

Although the data preparation phase is not defined in the EHDS regulation, some examples of good practice and processes that might help data holders are discussed below.

It is advisable to import the data first into a separate environment from the primary sources. This environment separated from production databases of the data holder enables to ensure that security, safety and privacy of the data is not directly compromised. Here we make a distinction between subset creation, data extraction and data harmonisation.

- **Subset creation**: The data subset creation is one of the more demanding activities that the data holder may have to perform. Frequently, the complete datasets offered by a data holder in the dataset catalogue is created on an ongoing basis by the data holders. It can be large and contain much more data than data users typically have been granted access to by the HDAB. See section 4.1.4 for more details on subset creation. Before creating the subset, the data holder must verify that the defined population and variables match the specifications in the data permit or approved data request. This ensures that only the relevant observations are included, since providing an incorrect subset could add data that is not included in the data permit or request approval.

- **Data extraction** refers to the process of collecting or retrieving varying types of data from a range of sources or a larger source of electronic health data. Data extraction ensures provisioning only the data that are requested by the data user and that are kept inside of a set of a larger source of electronic health data or multiple datasets of one data holder.

- **Harmonisation of data:** When a data permit contains data from multiple data sources, data holders may be asked to harmonise on topics such as naming convention, coding convention and formatting. This is both to facilitate easier data linkage and analysis of the provided data. However, performing data harmonisation is outside of mandatory duties of data holders. Data holders shall provide the data with the naming convention, coding and formats as described in the data catalogue. Though transformation of existing data into a cohesive, standardised format according to a schema convenient for data applicant may be useful for certain data analytic tasks, this kind of data processing should not be part of normal procedures for data permit or data request approval.

See checklist for EHDS health data holders on subset creation in Annex 6

Annex 5 Steps and illustrative checklist for data holders

The checklists in Annex 5 are illustrative and provide a non-exhaustive overview of recommended steps based on expert advise. The checklists do not extend in any way the rights and obligations deriving from applicable legislation nor introduce any additional requirements.

A5.1 Checklist for EHDS health data holders in preparation of the EHDS

1. **Determine Eligibility**
   ☐ Confirm whether your organisation qualifies as a *health data holder* under the EHDS (based on roles and types of data processed).
   ☐ For companies in categories on the verge of the applicability of Chapter IV of the EHDS regulation, check regularly at least once a year whether they meet the relevant requirements.

2. **Know Your Data Types and Categories**
   ☐ Classify your data: personal, non-personal, anonymised, synthetic, or mixed.
   ☐ Analyse your existing health data from the viewpoint of health data categories for which there is obligation for making them available.
   ☐ Understand EHDS obligations for each type and category of health data.

3. **Metadata & Dataset Description** (WP5 TEHDAS2)
   ☐ Prepare metadata using HealthDCAT-AP.
   ☐ Submit and annually update dataset descriptions in your national dataset catalogue.

4. **Data Provision & Timelines**
   ☐ Set up processes to provide data within the necessary time limits (Figure 4)
   ☐ Be able to deliver data via the HDAB and external Secure Processing Environments.

5. **Internal Capacity & Readiness**
   ☐ Assess your maturity level in data governance, quality, metadata management, and technical capability (Annex 3).
   ☐ Identify resource gaps and training needs.

6. **Follow National Implementation Rules**
   ☐ Monitor your Member State's EHDS-legal and technical architecture choices (e.g. opt-out system, HDAB setup, intermediation options).
   ☐ Be aware of relevant national legislation.
   ☐ Align with national legislation, procedures and exceptions.

7. **Handle Intellectual Property & Trade Secrets**
   ☐ Identify datasets containing IP/trade secrets.
   ☐ Notify HDAB via metadata of these trade secrets and request safeguards if needed.

8. **Trusted Data Holder Option**
   ☐ Consider applying to become a trusted data holder if you meet technical and legal requirements.

☐ If aspiring to become a trusted data holder: Understand the additional duties for the trusted data holder (e.g. evaluating data requests).

9. **Use of Intermediation Entities**

☐ If relevant: Explore delegating duties (like data processing) to a Health Data Intermediation entity, if allowed by national law.

☐ If relevant: Identify your Member State relevant HDIEs.

10. **Communication & Interaction with HDAB**

☐ Establish (secure) channels for formal and informal communications with the HDAB.

☐ Establish (secure) channels for formal and informal communications with the data user.

☐ Establish (secure) channels for formal and informal communications with the SPE.

11. **Cost Recovery & Invoicing**

☐ Understand which preparation costs are reimbursable.

☐ Provide justifications and estimates to HDABs in advance.

12. **Know where to find relevant information**

☐ Stay Informed with EHDS & TEHDAS2 Guidelines

☐ Follow TEHDAS2 for updates and guidelines relevant for data holders

☐ Follow HealthData@EU for updates on infrastructure and application procedures.

A5.2 Checklist for EHDS health data holders on subset creation

1. General

☐ Verify the following aspects of the HDAB´s request:

- **Scope**
- **Feasibility**
- **Timeframe**

☐ Review the data permit or data request approval to identify the required observations and variables.

☐ Confirm that a data subset is needed.

2. Understanding the Source Dataset

☐ Identify whether the data is from a single file or multiple data sources (e.g., EHRs, PACS, insurance datasets).

☐ Check if the source data contains more variables and individuals than needed

☐ Clarify if data extraction involves structured, unstructured, or combined data types

3. Subset Design and Data Consolidation

☐ Determine if the required subset can be created with the given variables and population criteria

☐ Ensure inclusion of only relevant data

☐ Perform data consolidation tasks including:

- Data subset creation,
- Duplicate elimination,
- Data quality control,
- Data linkage (if needed), with linkage quality assessment

4. Data Extraction

☐ Identify appropriate tools or methods for data extraction (manual, software-based, AI-powered).

☐ Limit extraction to only the approved and catalogued data items.

☐Respect opt-outs and handle any IP or trade secrets in the data.

☐ Ensure data remains consistent with naming, coding, and formatting conventions from the data catalogue.

☐ Validate dataset content and structure before delivery.

A5.3 Checklist for EHDS health data holders on Data Preparation

1. **General preparation**
   ☐ Understand whether you are responding to a data permit or a data request.
   ☐ Understand potential additional obligations for trusted data holders.
   ☐ Understand time limits for data preparation.
   ☐ Choose a data preparation sequence suited to your data type and internal workflows.

2. **Opt-out management** (if assigned to the data holder by national law)
   ☐ Check for justified exceptions to opt-out as defined by national law.
   ☐ Ensure only data from individuals who have not opted out is included.
   ☐ If unable to manage opt-out, notify the HDAB.

3. **IP and trade secrets management (if appliable)**
   ☐ Implement the approved technological or restrictive protection measures for IP or trade secret content.

4. **Data minimisation & purpose limitation**
   ☐ Include only data or datasets (population, time period, geographical area) explicitly reported in the data permit/request.
   ☐ Include only variables explicitly reported in the data permit/request, paying attention to the eventual transformations required by the HDAB to remove or generalise direct and indirect identifiers.

5. **Pseudonymisation & anonymisation**
   ☐ Apply anonymisation, unless the purpose of the data processing can only be achieved with pseudonymised data (in this case apply pseudonymisation).
   ☐ Where identifiable information must be provided, separate direct personal identifiers and health records and communicate to HDAB how to link the data.
   ☐ Use clear procedural and technical guidelines during the process of pseudonymisation.

6. **Data linkage**
   ☐ Apply data linkage if necessary, in order to combine several datasets or data from datasets.
   ☐ Use clear procedural and technical guidelines during the process of data linkage.

7. **Statistical aggregation in case of a data request**
   ☐ Follow detailed instructions in the data request approval to carry out statistical aggregation.
   ☐ If HDAB needs to handle opt-out or data linkage, transfer individual-level data to HDAB for final processing.

8. **Data inspection before delivery**

☐ No missing values where fields are expected to be filled.
☐ No duplicate rows or IDs
☐ No obvious input errors.
☐ Field names and formats match the data specification.
☐ Carry out optional data quality checks.

A5.4 Checklist for EHDS health data holders for providing data.

General Responsibilities

☐ Ensure data provision only follows an **approved data permit or request** specifying the purpose and access limitations.

☐ Determine the correct data flow based on:

- Type of application: **Data permit** or **Data request**
- Type of data: **Personal**, **non-personal open**, or **non-personal restricted data**
- Involvement of: **HDAB, SPE**, **data holder**, or **Intermediation Entity**

1. Data Permit Provision Flow

Starting point is when data is prepared

☐ Identify the SPE (HDAB or external) to which the data will be provided

☐ Contact HDAB or SPE to discuss where and how to deliver your data

☐ Attach metadata and dataset identifier to your dataset

☐ Encrypt data before transfer

☐ Share encryption key through a separate channel

☐ Respond to Data User or HDAB request for clarification or changes (modifications to the dataset)

☐ Support interaction with HDAB or health data user if necessary

2. Data Request Provision Flow (Two Options)

☐ Determine who performs the analysis (this can be either the health data holder, the health data intermediation entity (HDIE) or the HDAB)

Option 1: the HDAB or HDIE performs the analysis

☐ Provide individual-level data to the HDAB or HDIE for anonymised, statistical processing

☐ Follow the same data transfer steps as for a data permit (see above)

Option 2: Data Holder performs the analysis (applies also to data holders)

☐ Identify the location where to provide the results to

☐ Conduct analysis resulting in anonymised, aggregated data

☐ Provide results to HDAB or directly to the data user

☐ Add relevant metadata and versioning when needed

3. Provision of Non-Personal Data

☐ Determine whether you have open data (A) or restricted non-personal data (B)

A. Open Data

☐ Ensure your health data is findable in the national dataset catalogue.

☐ Make datasets accessible via a stable link to an open database

C. Restricted Access Non-Personal Data

☐ Ensure compliance with IP/sensitivity protections
☐ Add metadata and versioning
☐ Provide encrypted data using approved transfer method
☐ Share encryption key separately
☐ Respond to Data User or HDAB requests for clarifications or changes to the dataset if required

Annex 6 Data holder resources

A6.1 TEHDAS2 guidance

In the TEHDAS2 Joint action, many guidelines and specifications are provided for all roles in the EHDS regulation of which the target audience usually include the data holders. Many will provide useful information for data holders in their preparation for the EHDS.

- **M4.1.1 Guideline on fees related to the EHDS regulation.** This guideline helps stakeholders to understand the fee structure in the EHDS;
- **M4.1.2 Guideline on penalties for non-compliance related to the EHDS regulation.** This guideline helps stakeholders to understand the penalties for non-compliance structure in the EHDS;
- **M4.3 Guideline for Health Data Access Bodies on international and third country access and transfer of personal and non-personal electronic health data**. This guideline helps the data holder understand rules and infrastructure regarding international and third country access;
- **M5.1.1 Guideline for health data holders on data description, describing the data holders' duties regarding data description on Data discovery.** This guideline explains how to use HealthDCAT-AP to describe datasets and provides clear, practical steps to ensure metadata is accurate, interoperable, and compliant with legal requirements.
- **M5.1.2 Guidelines for HDABs on minimum categories and limitations on the reuse of health data.** This guideline helps the data holder understand which category they are, which is relevant for understanding whether they are health data holder under the EHDS regulation and for choosing the correct category when submitting their metadata;
- **M5.3 Guideline for Health Data Access Bodies on enrichment of health datasets.** This guideline helps (trusted) data holders in their data preparation phase by providing detailed information;
- **M 6.2 Guideline for data users on good application practice for data access and request.** This guideline supports data users in navigating the EHDS data application process by offering detailed instructions on identifying relevant datasets, meeting regulatory requirements, and fulfilling access and usage condition
- **M6.3 Guideline for Health Data Access Bodies on the procedures and formats for data access**. This guideline helps (trusted) data holder in understanding their role in the application assessment process by providing detailed information;
- **M7.2 Technical specification for Health Data Access Bodies on data minimisation and de-identification.** This guideline helps the (trusted) data holder in their data preparation phase by providing detailed information;
- **M7.3 Technical specification for Health Data Access Bodies on the implementation of the common IT infrastructure.** This specification helps the (trusted) data holder navigate the national and international IT-infrastructure;
- **M7.4 Technical specification for Health Data Access Bodies on the implementation of secure processing environments.** This specification helps the (trusted) data holder understand the requirements for providing the data to the SPE;

- **M7.5 Guideline for Health Data Access Bodies on linkage of health datasets.** This guideline helps the (trusted) data holder in their data preparation phase by providing detailed information;
- **M8.1 Guideline for Health Data Access Bodies on implementing opt-out from the secondary use of health data.** This guideline helps (trusted) data holder in their data preparation phase by providing detailed information;
- **M8.2 Guideline for Health Data Access Bodies on implementing the obligation of notifying the natural person on a significant finding from the secondary use of health data.** This guideline helps the data holder in understanding the potential interaction and processes regarding significant findings;
- **M8.3 Guidelines for Secondary Data Users on Handling Research Outcomes**, This guideline provides guidance on regulatory, ethical and legal considerations.

A6.2 HealthData@EU

HealthData@EU is the cross-border infrastructure supporting secondary use under the EHDS.[11]

The platform presents a gateway to the HealthData@EU Infrastructure and (once fully developed) will provide relevant information and the key services required by the European Health Data Space Regulation (such as Dataset Catalogue, Data Application Forms).

- It will 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.
- It is composed of elements operated by different actors.

As per EHDS regulation, in 2028 the HealthData@EU Central Platform will be fully operational. In the meanwhile, regular releases of the pre-deployment infrastructure are published and made available open source.

The HealthData@EU platform is useful for data holders in the preparation for the EHDS, as it provides detailed information on the future central service applications and most common infrastructure choices, which affects the data provision flows.

A6.3 QUANTUM

QUANTUM is an EU-funded project (2024-2026) that aims to create a common label system for Europe that guarantees the quality and utility of datasets for scientific and health innovation purposes[12]. This label system will enable researchers, policymakers, and healthcare professionals to identify high-quality data for research and decision making.

[11] HealthData@EU Central Platform. acceptance.data.health.europa.eu public

[12] Home - QUANTUM: The health data quality label

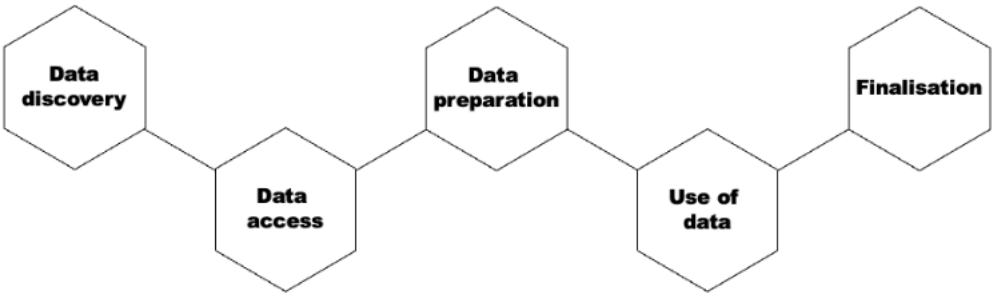
In the QUANTUM project:

- A quality and utility label is created to specify the data holders' data quality maturity,
- The label is tested with the data holders,
- Sustainable recommendations are provided for the HealthData@EU infrastructure, and
- A learning program is developed, setting up a long-lasting data quality community of practice where data holders can attain necessary knowledge on improving their data quality.

A6.4 Data user journey

When a data user[i] applies for electronic health data for secondary use purposes, such as research and innovation activities, education, and policy-making, within the European Health Data Space (EHDS), the user journey consists of several stages (see Figure 1). Access for certain purposes (public or occupational health, policy-making and regulatory activities, and statistics) is reserved for public sector bodies and Union institutions (see Chapter IV, Art. 53(1) and 53(2)).

Figure 1: EHDS user journey consists of five main phases: data discovery, data access, data preparation, use of data and finalisation.



Data discovery

Before being able to use the data, the user needs to investigate whether the data needed is available, and whether it is available in the necessary format for the secondary use purpose. This phase is called data discovery. Datasets available in the EU can be found in a metadata catalogue at https://qa.data.health.europa.eu/. Once the data discovery is completed, the user can begin the process of applying for the data.

Data access

In the data access phase, the user fills in and submits a dedicated and standardised data access application form or a data request to a health data access body (HDAB)[ii]. The user

must complete the information required in the form, upload necessary documents, and provide justifications as needed.

Data access application form is used when the user seeks to use personal level data. **Data request** is for cases when the user wants to apply for anonymised statistical data.

Data preparation

During this phase, the data holder(s)[iii] deliver(s) the necessary data to the HDAB, which starts to prepare the data for secondary use. Techniques for pseudonymisation, anonymisation, generalisation, suppression, and randomisation of personal data are employed. The data minimisation principle (as per the GDPR) must be respected to ensure privacy.

Use of data

In this phase, the user performs analyses based on the received data for the purpose defined in the application phase. Analysing personal level data must be performed in a secure processing environment[iv]. The duration of this phase is specified in the Regulation (Art 68(12)).

Finalisation

This last phase of the user journey concerns data user's duties regarding analysis outcomes derived from secondary use of data. Data user must publish the results of secondary use of health data within 18 months of the completion of the data processing in a secure processing environment or of receiving the requested health data. The results should be provided in an anonymous format. The data user must inform the health data access body of the results. In addition, the data user must mention in the output that the results have been obtained by using data in the framework of the EHDS.

Annex 7 Methodology

The contributors participated according to their promised commitments, ensuring a collaborative and thorough development process. See below the information about our structured work together.

- Desk research was performed by all contributors. During this process, relevant information was collected from expert organisations, related programmes and entities, such as the Community of Practice, QUANTUM, TEHDAS1.
- Working meetings − We conducted regular working meetings to discuss and outline the key components and structure of the guideline, as well as address any unclarities in the regulation.
- Write-a-thons − Nine write-a-thons, lasting two to three hours, were held to collaboratively draft and refine the content. What was not written during the write-a-thon was finished offline by a designated contributor.
- Artificial Intelligence (AI) tools were employed to support the development of this document, particularly OpenAI's ChatGPT. The enterprise environment of OpenAI was used, ensuring that no data entered was stored or used for training AI models. ChatGPT was used for summary and suggestive purposes. All output generated by ChatGPT was reviewed, edited, and finalised by the contributors. None of the text in the document was independently written by AI or LLM.
- Consultations with DG SANTE − Four meetings with representatives from DG SANTE were organised to ensure alignment with regulatory requirements and to gather expert feedback.
- Consultations with related TEHDAS2 tasks in which alignments between the guidelines was ensured.