Milestone 7.3: Draft Technical specifications for Health Data Access Bodies on the implementation of the common IT infrastructure

TEHDAS2 - Second Joint Action Towards the European Health Data Space

17 September 2025

Co-funded by
the European Union

0 Document info

Disclaimer
Views and opinions expressed in this deliverable represent those of the author(s) only and do not necessarily reflect those of the European Union or HaDEA. Neither the European Union nor the granting authority can be held responsible for them.

1.1 Authors

Author(s)	**Organisation**
Sylla M'Bemba	Health Data Hub, France
Brinkmann Pia	Bfarm, Germany
Dudova Zdenka	Masaryk University, Czech Republic
Kobekova Alexandra	Bfarm, Germany
Lähteenmäki Jaakko	VTT, Finland
Prentzas Nicoletta	University of Cyprus, Cyprus
Skovgaard Svingel Lise	Aarhus University, Denmark
Reviewers	**Organisation**
Pradeilhes Jean-Marie	Health Data Hub, France
Jendrossek Mario	Health Data Hub, France
Schäfer Amélie	Health Data Hub, France
Alvarez Minerva	Ministry of Health, Spain
Gütter Zdenek	Ministry of Health, Czech Republic
Holub Petr	Masaryk University, Czech Republic
Kristiansen Olav Astad	Norwegian Directorate for e-Health, Norway
Martin Anna	Ministry of Health, Spain
Schneider Katharina	Health Data Hub, France
Stachurski Tomasz	CeZ, Poland
Van Meerendonk Peter	Nictiz, Netherlands

1.2 Keywords

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

1.3 Document history

Date	Version	Editor	Change	Status
27/05/2025	0.1	M'Bemba Sylla	Initial document creation	Draft
03/06/2025	0.2	Authors and Contributors	First draft MS structure	Draft
16/06/2025	0.3	Authors and Contributors	First draft of the MS	Draft
24/06/2025	0.4	Authors and Contributors	First draft reviewed	Draft
30/06/2025	1	Amélie Schäfer and M'Bemba Sylla	Final version before Consortium Review	Final
31/07/2025 & 03/09/2025	1.1	EC review & Consortium review	New draft version during public consultation	Draft
05/09/2025	2	Final version	Final version after Consortium & EC Review	Final

Accepted in Project Steering Group on 12 September 2025.

Copyright Notice

Contents

1 Abbreviations

Term	Abbreviation
Applicability Statement 4	AS4
Application Programming Interface	API
Community of Practice	CoP
Create, read, update, and delete	CRUD
Create, update, and delete	CUD
Deliverable	D
Data Catalogue Vocabulary Application Profile	DCAT-AP
Data Governance Act	DGA
Directorate-General for Digital Services	DIGIT
Electronic Health Record	EHR
European Health Data Space	EHDS
European Union	EU
General Data Protection Regulation	GDPR
Health Data Access Body	HDAB
Health Data Catalogue Vocabulary Application Profile	HealthDCAT-AP
Interoperability Testbed	ITB
Joint Action	JA
Key Performance Indicator	KPI
Multifactor authentication	MFA
National Contact Point	NCP
Resource Description Framework	RDF
Secure Processing Environment	SPE
The Finnish Innovation Fund	Sitra
Simple Object Access Protocol	SOAP
Statistical Data Catalogue Vocabulary Application Profile	StatDCAT-AP
Towards the European Health Data Space	TEHDAS
Uniform Resource Identifier	URI
Work Package	WP

2 Executive summary

2.1 HealthData@EU infrastructure

Efficient and secure cross-border access to health data for secondary purposes such as research, innovation, policymaking, and improving patient safety is of strategic importance for the European Union. However, today, technical fragmentation and varied national frameworks hinder seamless secondary use of data among EU Member States.

To overcome these challenges, Chapter IV of the European Health Data Space (EHDS) regulation introduces a dedicated common EU infrastructure: HealthData@EU. This infrastructure provides the necessary technical, functional, and security frameworks to enable secure and standardised secondary use of electronic health data across national borders.

The HealthData@EU infrastructure and the HealthData@EU Central Platform, are defined as follows:

- HealthData@EU infrastructure: the infrastructure connecting national contact points for secondary use of electronic health data with the HealthData@EU Central Platform
- The HealthData@EU Central Platform for secondary use of electronic health data: the interoperability platform established by the European Commission to support and facilitate the exchange of information between national contact points for secondary use of electronic health data.

The HealthData@EU infrastructure and central platform must be able to communicate securely with all authorised participants of HealthData@EU, as defined under article 75(2) of the EHDS regulation.

This communication is enabled by specialised software that ensure secure exchange of information between health data access bodies. The solutions guarantee that data is encrypted, access is authenticated and authorised, and compliance with data protection regulation sur as GDPR is maintained, thus protecting the confidentiality and integrity of health data.

As specified in Article 75 of the EHDS regulation, the European Commission holds the primary responsibility for developing, maintaining, and continuously improving the HealthData@EU infrastructure. This responsibility includes proposing robust interoperability standards, consistent data exchange protocols, and secure data-sharing mechanisms tailored to the secondary use context.

At the national level, Member States contribute by deploying and managing national contact points for secondary use of electronic health data (NCPs), acting as connectors between their national data environments and the HealthData@EU infrastructure. NCPs ensure reliable national integration with relevant services such as the national dataset catalogue or the data access application management system, maintaining compliance with standards and facilitating secure data flows.

Together, the HealthData@EU Central Platform, the HealthData@EU infrastructure (managed by the European Commission) and national implementations coordinated via NCPs establish a comprehensive, interoperable, and secure environment. This robust infrastructure, once fully operational, should significantly enhance the EU's ability to leverage health data for secondary purposes, fostering cross-border collaboration and driving collective health research and policy advancements across Europe.

This document provides the outcome of the task 7.3 under the TEHDAS2 Joint Action. It aims to present a policy-level overview of the proposed common IT infrastructure supporting the HealthData@EU infrastructure, with a focus on cross-border connectivity and system interoperability. The content is based on the technical specifications and architecture [1] developed by the European Commission. It has been adapted to support public consultation and prepare Member States for implementation in alignment with Chapter IV of the EHDS regulation.

3 Background information

3.1 The TEHDAS2 Objectives

Advancing health data use in the European Health Union

As part of the work on 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, 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 data holders, data users and the new Health Data Access Bodies (HDABs) in fulfilling their responsibilities and obligations outlined in the European Health Data Space (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 (SPE): 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 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.

The work performed in Work package 7 (WP7) addresses “Safe and secure processing” of electronic health data within the EHDS infrastructure. The goal is to enable secure processing of EU citizen's electronic health data while fostering a secure, interoperable, and efficient health data ecosystem. The output of this work package consists of guidelines and technical specifications that shall inform further decisions and technical frameworks to set up the EHDS.

The results of WP7 are distributed across five tasks. Task 7.1 provides guidance to users about their duties and responsibilities when analysing data in a secure processing environment. Next, guidelines for data minimisation and de-identification give directions on how to address the challenges of health data minimisation, pseudonymisation, anonymisation and the generation of synthetic data (task 7.2 includes sub-tasks: 7.2.1, 7.2.2, 7.2.3 & 7.2.4). Specifications for the implementation of a common IT infrastructure (task 7.3) shall help member states to connect to the EHDS ecosystem. To ensure interoperability, common security requirements applicable to all secure processing environments are defined in addition to functional and technical services that should be part of all secure processing environments (task 7.4). Lastly, information about data linkage techniques and possibilities of quality control of linked data are collected (task 7.5).

Here is an overview of the documents that are part of WP7:

1. Guidelines for data users on how to use data in a secure processing environment (task 7.1);
2. Guidelines for Health Data Access Bodies on data minimisation, pseudonymisation, anonymisation and synthetic data (task 7.2);
3. Technical specifications for Health Data Access Bodies on the implementation of the common IT infrastructure (task 7.3);
4. Technical specifications for Health Data Access Bodies on the implementation of secure processing environments (task 7.4);
5. Guidelines for Health Data Access Bodies on linkage of health datasets (task 7.5).

3.2 Relevant provisions of the EHDS regulation

The legal foundation for the HealthData@EU infrastructure is set out in Chapter IV of the EHDS regulation, which establishes the framework for enabling the secure and interoperable secondary use of electronic health data across the EU.

Article 75 defines the scope and governance of the common infrastructure for secondary use. It tasks the European Commission with developing and operating the central services of HealthData@EU and mandates the adoption of common technical and organisational requirements. It also requires each Member State to establish an NCP to ensure secure connectivity to the EU-level infrastructure. Furthermore, Article 75 acknowledges the involvement of additional actors such as the Union Health Data Access Body and other authorised participants (including certain European or international research infrastructures) which may also connect to the HealthData@EU under defined conditions.

While not legally binding, Recital 80 provides essential interpretive context to Article 75. It emphasises the need for an inclusive and sustainable cross-border infrastructure that respects privacy-by-design principles, facilitates discoverability, and supports technical and organisational gateways via NCPs. It also recognises the possibility of linking health data with other European data spaces (e.g. environment, agriculture) to gain insights into health determinants.

Together, these articles form the regulatory backdrop for the milestone 7.3, which aims to define the technical specifications enabling national infrastructures to connect with the HealthData@EU Central Platform. In line with the March 2025 agreement between WP leaders and the European Commission, this document takes the form of a policy-level document based on Release 4 documentation [1], designed to simplify the available documentation.

3.3 Timeline of development of the HealthData@EU infrastructure

The development of the HealthData@EU infrastructure has progressed through several phases, reflecting a stepwise approach to designing, testing, and preparing the common infrastructure for the secondary use of health data across the EU.
Initial exploratory work was conducted as part of the HealthData@EU Pilot Project, which tested the feasibility of cross-border data sharing and explored early governance and technical models. This pilot project provided valuable insights into practical implementation challenges and laid the groundwork for the infrastructure's future design, delivering an Architecture Definition Document [6].

Since 2023, the European Commission’s DG SANTE has coordinated the development of successive releases of the HealthData@EU infrastructure and Central Platform which are available here. These iterative releases aim to ensure technical maturity, stakeholder readiness, and regulatory coherence.

In parallel, the TEHDAS2 Joint Action [5] plays a strategic role in supporting implementation by producing detailed technical specifications and policy guidelines. It helps align Member States and stakeholders around a shared operational model and promotes common understanding of roles, responsibilities, and infrastructure requirements.

Within this context, the milestone 7.3 provides a consolidated policy-level summary of the infrastructure’s status as for Q2 2025. It aims to support Member States in their preparation for connecting to the HealthData@EU infrastructure and contributes to the overall effort of ensuring consistency, interoperability, and readiness ahead of formal deployment.

4 Scope of the HealthData@EU Infrastructure

The objective of this document is to present the technical layer of the HealthData@EU infrastructure and the use cases for which it was developed. The HealthData@EU infrastructure enables secure and interoperable data exchange between Member States and authorised participants Contact Points and the HealthData@EU Central Platform.

4.1 In-Scope

This includes key technical components required to enable cross-border connectivity and conformance for secondary use of health data, as foreseen in Article 75 of the EHDS regulation. It includes the following key components:

- **National Contact Points (NCPs):** National gateways designated by Member States with deployed business and messaging solution of the HealthData@EU infrastructure.

- **National and Central Dispatchers:** Technical components that manage and route messages between national infrastructures and the HealthData@EU Central Platform, ensuring secure and traceable communication.

- **eDelivery (Domibus):** The EU-endorsed secure messaging protocol used for routing and delivery of metadata and application messages between NCPs and the Central Platform.

- **The HealthData@EU Central Platform:** Platform operated by the Commission and offering the features requested by the EHDS regulation.

4.2 Out of scope

This milestone does not cover aspects beyond the common infrastructure layer required to enable cross-border connectivity and conformance.

Elements excluded from the defined scope include, without limitation, the following:

- **Detailed user interface designs:** Visual design, layout, and front-end specifications for portals or dashboards used by stakeholders are excluded.

- **Member State-specific modules or extensions:** National adaptations, internal workflows, or system components that do not impact cross-border interactions are not addressed.

- **Detailed architecture and technical specifications of the HealthData@EU Central Platform:** The official documentation of each release of the Central Platform is made available by the Commission as publication in the Official Journal.**.**

- **Low-level technical implementation details:** This document does not define infrastructure deployment configurations, source code, or runtime specifications. These elements will be handled at later technical stages or by implementing bodies.

The focus remains on presenting a clear, functional-level view of the shared infrastructure to support interoperability and alignment across Member States and HealthData@EU Central Platform.

5 HealthData@EU infrastructure stakeholders and use cases

5.1 The HealthData@EU infrastructure stakeholders

This section focuses on the technical infrastructure stakeholders, and not on the full list of actors involved in the HealthData@EU infrastructure.

The key infrastructure stakeholders involved in enabling secure cross-border secondary use of electronic health data in the distributed HealthData@EU infrastructure are the:

- NCPs for secondary use, operated by each Member State,
- HealthData@EU Central Platform, operated by the Commission.

For each Member State, the NCP for secondary use acts as the interface between national services and the cross-border HealthData@EU infrastructure. To enable this role, the NCP must deploy the following components:

- the HealthData@EU National Dispatcher
- the National eDelivery Access Point

For the HealthData@EU Central Platform to be able to exchange the information with NCPs, the Commission must deploy:

- the HealthData@EU Central Dispatcher
- the Central eDelivery Access Point.

5.2 The HealthData@EU infrastructure use cases

The Release 4 *Business Requirements and Use Cases* [2] document presents several scenarios illustrating the potential use of the HealthData@EU infrastructure from various perspectives (e.g., as the HealthData@EU Central Platform, as NCP, or in interactions between the two).
Below is a non-exhaustive list, intended to provide an overview of possible uses within a connectivity framework. Member States are encouraged to consult the referenced document during their onboarding process or when actively using the infrastructure.

NB: The HealthDCAT-AP term used in the next sections refers to the EU's potential format for the common metadata framework.

Use cases for Dataset management

I. Create Dataset Request

II. Update Dataset Request

III. Delete Dataset Request

Use cases for Application lifecycle

IV. Data Access Application Form Exchange

V. Data Request Application Form Exchange

VI. Communication between data applicant and application assessors

VII. Update of submitted applications

Use cases for Decision Outcomes

VIII. Create positive decision for data access application - Data Permit

IX. Create negative decision for data access application

X. Create positive decision for data request application

XI. Create negative decision for data request application

Use cases for Appeals and reporting

XII. Create appeal from negative decision

XIII. Create Biennial Report of Health Data Access Body

XIV. Create Analysis study record

XV. Create sanctions and penalties record

The detailed message exchange flow for the use cases initiated by NCP is described in the Chapter 7.1 of this document. The message exchange flow is the same regardless of the content of the message (use case).

6 Components of the HealthData@EU infrastructure

The infrastructure is composed of two key layers:

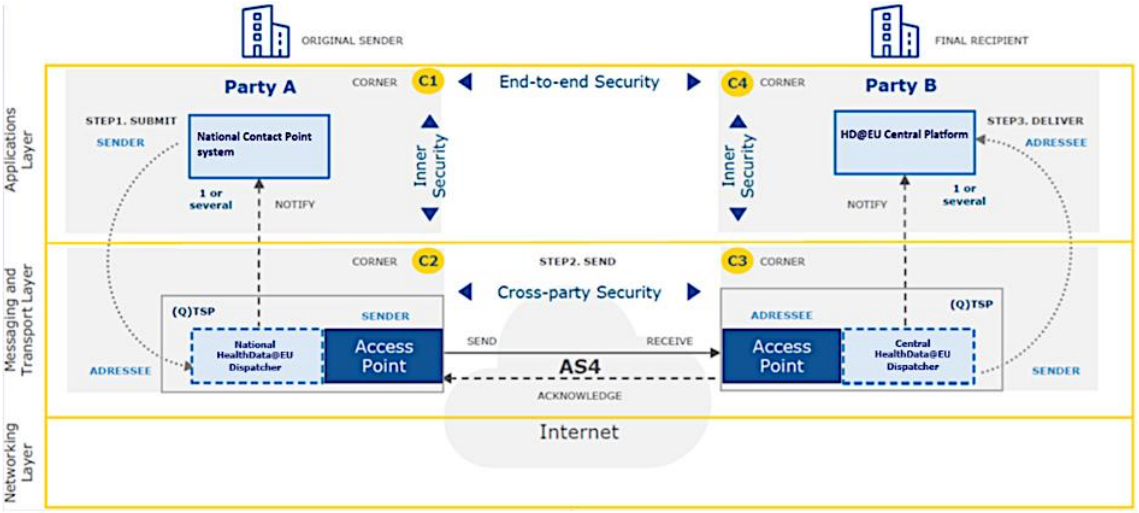
1. Business layer – responsible for managing message content and format.
2. Messaging (Transport) layer – responsible for the secure exchange of messages.

The HealthData@EU infrastructure enables secure, structured communication between NCP and HealthData@EU Central Platform supporting cross-border use of health data for secondary use. This infrastructure is distributed: some components are operated by the European Commission, while others are implemented and maintained by each Member State.

These components together enable point-to-point connections between each Member State and the HealthData@EU Central Platform, in line with the requirements of **Article 75** of the EHDS regulation, which mandates each Member State to designate a National Contact Point for secondary use. The names and functions reflect the current technical design (Release 4) and do not themselves constitute legal obligations unless specified in implementing acts.

The following diagram presents a high-level overview of the HealthData@EU infrastructure.

Figure 1: An illustration of the four-corner model of the HealthData@EU infrastructure



Source: HealthData@EU Central Platform, Open-source release 4: objectives, business requirements and use cases, IUC Figure 1

For an NCP to be able to join the HealthData@EU infrastructure, the below technical components must be deployed:

- National HealthData@EU Dispatcher - **Business layer** - ensures that the data exchanged between national and central system comply with the HealthData@EU business and technical requirements.
- National eDelivery Access Point - **Messaging layer** - ensures secure message transport between national and central system.

For the HealthData@EU Central Platform to be able to join the HealthData@EU infrastructure, the below technical components must be deployed:

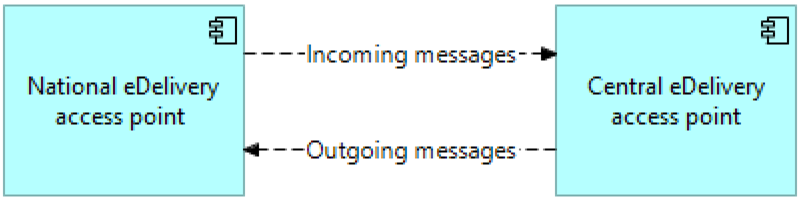
- Central eDelivery Access Point - **Messaging layer** - ensures secure message transport between national and central system.
- HealthData@EU Central Dispatcher - **Business layer** - ensures that the data exchanged between national and central system comply with the HealthData@EU business and technical requirements.

All communication between NCPs and the HealthData@EU Central Platform is point-to-point, with no direct connections between Member States. This means:

- HealthData@EU National Dispatchers and National eDelivery Access Points communicate only with the HealthData@EU Central Platform.
- There is no peer-to-peer exchange between NCPs or national systems from different Member States.

The European Commission’s eDelivery building block is used to send messages between the HealthData@EU central platform and the NCPs (Figure 2). Messaging is based on ebMS3 (ebXML Messaging version 3.0) standard of OASIS and its payload-agnostic AS4 Conformance Profile. European Commission maintains a reference implementation (“Domibus”) of an AS4 Access Point. Domibus has been used as a component of the central platform and is also recommended for use in NCP implementations. However, other compatible solutions are also authorised.

Figure 2: Messaging between a National Contact Point and the HealthData@EU Central Platform


National eDelivery access point
Incoming messages
Outgoing messages
Central eDelivery access point

7 Messages exchange through the HealthData@EU infrastructure

7.1 Regulatory provisions

The messages flow through the HealthDataEU infrastructure was designed to fulfil the EHDS regulatory provisions (Articles 75 and 76). Details related to information flows and corresponding HealthData@EU Central Platform functions/support are presented in the table below.

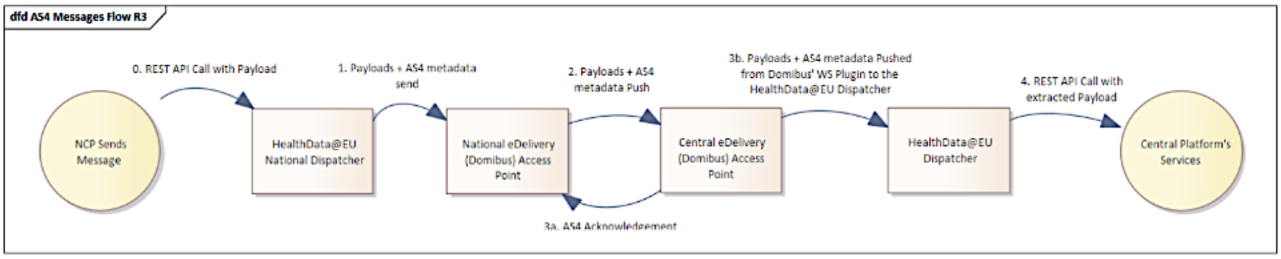
Table 1: EHDS regulation provisions related to messages exchange.

Regulation	HealthData@EU Central Platform functions/support
Secure communication infrastructure: The regulation mandates the use of secure and interoperable communication infrastructure.	Implementing eDelivery Access Point as Messaging layer in the HealthData@EU infrastructure.
Interoperability and standardisation: The regulation imposes requirements for semantic and technical interoperability.	Implementing HealthData@EU Dispatcher as Business layer in the HealthData@EU infrastructure.
EU Dataset Catalogue Synchronisation: NCPs must ensure that information about available electronic health datasets is continuously and systematically provided to the HealthData@EU infrastructure, using a common metadata format to be defined.	HealthData@EU Central Platform is responsible for receiving dataset metadata from Member State via HealthData@EU infrastructure.

Cross-border data access mechanisms: The regulation introduces a pan European mechanism for data users in one Member State to request access to datasets datasets **held** in another Member State, requested in the HealthData@EU Central Platform and coordinated via the NCPs and HDABs.	HealthData@EU Central Platform is responsible for distributing such requests to relevant NCPs of Member State.

7.2 Message exchange implementation

Figure 3: HealthData@EU infrastructure Message Flow


dfd AS4 Messages Flow R3
0. REST API Call with Payload
1. Payloads + AS4 metadata send
2. Payloads + AS4 metadata Push
3b. Payloads + AS4 metadata Pushed from Domibus' WS Plugin to the HealthData@EU Dispatcher
4. REST API Call with extracted Payload
NCP Sends Message
HealthData@EU National Dispatcher
National eDelivery (Domibus) Access Point
Central eDelivery (Domibus) Access Point
HealthData@EU Dispatcher
Central Platform's Services
3a. AS4 Acknowledgement

Source: HealthData@EU Central Platform, Open-source release 4: architecture model and technical specification, Figure 7

The message exchange was implemented in the same manner for all the use cases listed in chapter 5.1.

Message exchange flow for the use cases initiated by the NCP:
The NCP sends a chosen content of the message (based on business rules) to the National Dispatcher.

1. Validation and Preparation by National Dispatcher
   The National Dispatcher validates the conformance of the message, utilizing the HealthData@EU Interoperability Test Bed Validator and, if successful, prepares the message for transmission to the Central eDelivery Access Point.
2. The National Dispatcher forwards prepared message to the National eDelivery Access Point.
3. National eDelivery Access Point sends the message to the Central eDelivery Access Point. This secure transmission is handled by eDelivery Access Point. e.g., Domibus, where message is encrypted and signed with the national certificate.
4. The message is processed by Central eDelivery Access Point
   - Message status is updated to “RECEIVED”

- The message is decrypted
- The authenticity is validated
- The message is forwarded to the Central Dispatcher
- Status is updated to "DELIVERED"
- A digitally signed acknowledgment is sent back to the National eDelivery Access Point

5. The message is sent to Central Dispatcher.
6. Central Dispatcher validates the message conformance with business rules:
    - The Central Dispatcher validates the conformance of the message using the HealthData@EU Interoperability Test Bed
    - For security, the AccessPointID and the NationID of the sender is added to the payload
    - For traceability, the original MessageID is added to the payload
    - The payload is forwarded to the Central Platform Hub Repository
7. Processing by the Central Platform Hub Repository
    - The HealthDCAT-AP record is stored and associated with the respective NationID - this results in publishing the dataset in the Central Catalogue
    - The action is logged for auditing purposes
8. Central Platform Hub Repository Notifies an outcome to the Central Dispatcher.
    - The repository sends the outcome (success or failure with an error message) back to the Central Dispatcher. The Dispatcher prepares a response message by referencing the original MessageID.
9. The response message is sent back from the Central eDelivery Access Point to National eDelivery Access Point.
10. The message is stored by the National eDelivery Access Point. An event notification can inform the National Dispatcher that a message was received.
11. The National Dispatcher retrieves the message either via event trigger or through regular polling.
12. The National Dispatcher unwraps the response and stores it. The response is delivered to the NCP either via push or pull, depending on the national preference.

8 HealthData@EU End-2-end Test Framework

The Interoperability Test Bed (ITB) is a Commission-hosted tool designed to support voluntary conformance testing. While not legally required under the EHDS regulation, it facilitates the implementation of technical and organisational requirements pursuant to Article 75. In the context of HealthData@EU, it enables implementers (Member States and authorised actors) to verify that their systems conform to the messaging protocols, API behaviours, and data structures defined in the common infrastructure specification.

Test scenarios are grouped into test suites, each covering specific interaction patterns, such as:

- publication of dataset metadata to the EU Dataset Catalogue,
- submission and routing of access requests,
- response message handling.

The Test Bed operates through a self-service model: users are provided with access credentials and can execute validation tests independently. Results are delivered in real time and include detailed feedback, allowing implementers to detect and correct non-conformities before connecting to the live infrastructure.

The use of the Test Bed is optional, but it is recommended for all parties developing components that connect to the central platform, especially NCPs and organisations exposing dataset catalogues. The tool improves implementation quality, reduces integration delays, and ensures readiness for production onboarding.

Further information and user guidance are available in the dedicated documentation [3] provided with the infrastructure fourth release.

9 References

[1] Release 4 Technical Specification
[2] Release 4 Business Requirements and Use cases
[3] Release 4 Test Framework end-to-end tests
[4] http://data.europa.eu/eli/reg/2025/327/oj
[5] https://tehdas.eu/
[6] HealthData@EU pilot project - Deliverable 5.1 Architecture Definition Document

10 List of Annexes

Annex number	Annex title
1	Related legal framework
2	Business and technical requirements
3	ITB Use Case 3.0 - Validate Conformance with the HealthData@EU Infrastructure
4	Methodology
5	User Journey
6	Glossary

10.1 Annex 1 - Related legal framework

Table 2: Primary relevant articles for this milestone include (not limited):

EHDS regulation articles	Key relevant parts
Recital 80 - Establishment and principles of HealthData@EU (excerpts)	• “A cross-border infrastructure should be established (‘HealthData@EU’).” • “HealthData@EU should accelerate secondary use while increasing legal certainty, respecting the privacy of natural persons and being interoperable.” • “Member States should designate national contact points for secondary use […] and connect those contact points to HealthData@EU.” • “The Union health data access service should also be connected to HealthData@EU.”

EHDS regulation articles	Key relevant parts
	• "Authorised participants […] such as ERICs, EDICs, EOSC nodes, or international organisations […] may connect to HealthData@EU." • "The Commission could provide services including: exchange of information between HDABs and authorised participants, maintaining catalogues, connectivity, compliance services, and network discoverability." • "A secure processing environment […] could be set up by the Commission, allowing data from different national infrastructures to be transmitted and analysed." • "Existing systems for data sharing should be reused as much as possible […] such as those under the 'once-only' technical system."
Article 57 - Tasks of health data access bodies (selection)	(a)(i) Provide access to electronic health data "to health data users pursuant to a data permit in a secure processing environment in accordance with Article 73." (a)(ii) Monitor and supervise compliance "by health data users and health data holders with the requirements laid down in this regulation." (a)(iii) Request electronic health data "from relevant health data holders pursuant to a data permit issued or a health data request approved." (e) Maintain a management system to record and process: • health data access applications and requests, • decisions and data permits, • metadata including: applicant name, purpose, issuance date, permit duration, and application description. (g) Cooperate "at Union and national level to lay down common standards, technical requirements and appropriate measures for accessing electronic health data in a secure processing environment." (h) Provide advice to the Commission "on techniques and best practices for secondary use and the management of electronic health data." (i) Facilitate "cross-border access to electronic health data for secondary use […] through HealthData@EU referred to in Article 75."

EHDS regulation articles	Key relevant parts
	(j)(i) Make public "a national dataset catalogue that includes details about the source and nature of electronic health data" in line with Articles 77, 78, and 80. (j)(ii) Make public "any health data access application and health data request without undue delay after initial reception." (j)(iii) Make public "all data permits issued or health data requests approved as well as refusal decisions, including their justification, within 30 working days."
Article 67 - Health data access applications	(3) "When seeking access to electronic health data held by health data holders established in more than one Member State or from the relevant authorised participants in HealthData@EU referred to in Article 75, the health data applicant shall submit a single health data access application through the health data access body of the Member State where the main establishment of the health data applicant is located, through the health data access body of the Member State in which one of those health data holders is established or through the services provided by the Commission in HealthData@EU referred to in Article 75."
Article 68 - Data permit	(3) "Where the health data access body concludes that the requirements in paragraph 1 are fulfilled […] the health data access body shall grant access to electronic health data by issuing a data permit." "Health data access bodies shall refuse all health data access applications where the requirements in this Chapter are not fulfilled." (4) "The health data access body shall issue or refuse a data permit within three months of receiving a complete application." "If the application is incomplete […] the applicant shall be given four weeks to complete it." (5) "When handling a cross-border application […] HDABs and authorised participants in HealthData@EU […] shall remain responsible for adopting decisions […]" "They may take that information into consideration […] A data permit issued by one HDAB may benefit from mutual recognition." (8) "HDABs and authorised participants in HealthData@EU […] may decide to provide access in the secure processing environment provided by the Commission as referred to in Article 75(9)."

EHDS regulation articles	Key relevant parts
	(10) When issuing a data permit, the following must be included (technical relevance only): • (a) Data categories, format, sources, and indication if data is pseudonymised • (d) Identity of authorised users (e.g. principal investigator) • (e) Duration of the permit • (f) Technical tools/resources available in the secure processing environment
Article 70 - Templates to support access to electronic health data for secondary use	"By 26 March 2027, the Commission shall, by means of implementing acts, set out the templates for the health data access application, the data permit and the health data request referred to in Articles 67, 68 and 69, respectively. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 98(2)."
Article 75 - HealthData@EU	(1) Each Member State shall designate one national contact point for secondary use. “That national contact point […] shall be an organisational and technical gateway […] in a cross-border context.” (3) The national contact points and the Union health data access service shall connect to the cross-border infrastructure for secondary use, “namely HealthData@EU”. “They shall facilitate the cross-border access […] and cooperate closely with each other and with the Commission.” (6) Each national contact point and authorised participant shall: “Acquire the required technical capability to connect to and participate in HealthData@EU.” “They shall comply with the requirements and technical specifications needed to operate HealthData@EU and to allow them to connect to it.” (7) The Member States and the Commission shall: “Set up HealthData@EU to support and facilitate the cross-border access to electronic health data for secondary use […]” (8) The Commission shall: “Develop, deploy and operate a central platform for HealthData@EU by providing information technology services […]” “The Commission shall only process electronic health data on behalf of the controllers as a processor.”

EHDS regulation articles	Key relevant parts
	(9) “Where requested by two or more national contact points, the Commission may provide a secure processing environment […] compliant with Article 73.” If multiple NCPs or authorised participants submit data to this environment, “they shall be joint controllers and the Commission shall be processor.” (12) By 26 March 2027, the Commission shall adopt implementing acts to define: • (a) “Requirements, technical specifications and the IT architecture of HealthData@EU” ensuring security and confidentiality • (b) Conditions and compliance checks to join or remain connected • (c) Minimum criteria for national contact points and authorised participants • (d) Responsibilities of controllers and processors in HealthData@EU • (e) Responsibilities for the secure processing environment • (f) “Common specifications for the architecture of HealthData@EU and for its interoperability with other common European data spaces”
Article 79 - EU dataset catalogue	(1) “The Commission shall establish an EU dataset catalogue connecting the national dataset catalogues established by the health data access bodies in each Member State as well as the dataset catalogues of authorised participants in HealthData@EU.” (2) “The EU dataset catalogue, the national dataset catalogues and the dataset catalogues of authorised participants in HealthData@EU shall be made publicly available.”
Article 96 - Roles and responsibilities of the Commission regarding the functioning of the EHDS	(1) “[...] the Commission shall develop, maintain, host and operate the infrastructures and central services required to support the functioning of the EHDS, for all relevant connected entities”, by means of: • (e) “A service to submit health data access applications […] and to automatically forward the health data access applications to the relevant contact points, in accordance with Article 67(3).” • (f) “The central services and infrastructures of HealthData@EU, in accordance with Article 75(7) and (8).” • (g) “A secure processing environment, in accordance with Article 75(9), in which health data access bodies can decide to make data available.”

EHDS regulation articles	Key relevant parts
	• (h) "Compliance checks for connecting authorised participants to HealthData@EU." • (i) "A federated EU dataset catalogue connecting the national dataset catalogues, in accordance with Article 79." (2) "The services referred to in paragraph 1 of this Article shall meet sufficient quality standards in terms of availability, security, capacity, interoperability, maintenance, monitoring and development to ensure the EHDS functions effectively."

10.2 Annex 2 - Business and technical requirements

10.2.1 Business Requirements

The business requirements are divided into two types, for:

1. Users of the HealthData@EU Central Platform.

2. National Contract Points connection with HealthData@EU Central Platform (machine to machine requirements to exchange eDelivery messages).

Table 3: Users' requirements

User type	Requirement
General public	Need to be able to access the central platform
General public	Need to be able to choose the language of the central platform
General public	Need to be able to easily navigate between different functionalities of the central platform
General public	Need to be able to display and search metadata catalogue
General public	Need to be able display and search analysis results
Data user	Need to be able to identify, authenticate and get authorisation
Data user	Need to submit the data access and request applications
Data user	Need to monitor the status of the above requests
Data user	Need to amend the application
Administrator	Need to define, manage, generate reports, and use dashboard for Key performance indicators
Administrator	Need to analyse the HDAB Annual reports
Administrator	Need to have access to monitoring and logging of the platform

Table 4: Machine to machine requirements to exchange eDelivery messages

Machine need	Requirement
NCP	Need to send to Central Platform message with Create, Update, Delete (CUD) dataset records.
Central Platform	Need to send back to NCP the message if CUD message was or wasn't validated.
Central Platform	Need to send to NCPs the message containing Application.

Machine need	Requirement
NCP	Need to send back to Central Platform the message if the message containing Application was or wasn't validated.
Central Platform	Need to send to NCPs the message containing amended Application.
NCP	Need to send back to Central Platform the message if the message containing amended Application was or wasn't validated.
NCP	Need to send to Central Platform the messages with the status of the Application.
Central Platform	Need to send back to NCP the message if the message with status of the application was or wasn't validated.
Central Platform	Need to send to NCPs affected the message with the status of the application.
NCP	Need to send back to Central Platform the message if the message with the status of the application was or wasn't validated.
NCP	Need to send to Central Platform the message containing analysis results.
Central Platform	Need to send back to NCP the message if the message containing analysis results was or wasn't validated.
NCP	Need to send to Central Platform the message containing information about granted permits.
Central Platform	Need to send back to NCP the message if the message containing information about granted permits was or wasn't validated.
NCP	Need to send to Central Platform the message containing the information about penalties.
Central Platform	Need to send back to NCP the message if the message containing information about penalties was or wasn't validated.
NCP	Need to send to Central Platform the message containing the HDAB biennial report.
Central Platform	Need to send back to NCP the message if the message containing the HDAB biennial report was or wasn't validated.

10.2.2 Technical Requirements

In this section, the technical requirements are described for the HealthData@EU Central Platform and infrastructure.

Table 5: Technical Requirements and Traceability

Level	Requirement
System	The Central Platform must be compliant with the GDPR data privacy regulation
System	The Central Platform’s architecture and components shall be designed to ensure flexibility in deployment, enabling installation on AWS cloud platform.
System	The Central Platform shall generate logs allowing to be monitored and viewed by the deployment platform’s infrastructure
System	The Central Platform shall use a modular architecture.
System	The Central Platform shall implement microservices to ensure scalability and flexibility of operations.
System	The Central Platform’s microservices shall communicate via RESTful APIs or through shared persisted data
System	The Central Platform shall be deployable on latest x86/am64 GNU/Linux operating systems.
System	The Central Platform shall support authentication via EULogin and authorization using Keycloak
System	The Central Platform shall load within 3 seconds for 95% of users
System	The Central Platform shall use eDelivery as a gateway to connect with national nodes.

Level	Requirement
System	The Central Platform shall provide a web User Interface
Data Access Application	The Central Platform shall persist in a database Data Access Applications
Data Access Applications	The Central Platform shall persist in a database Status and Data Permits that result from a Data Access Application
Data Access Application	The Central Platform shall allow selecting multiple Distributions to be included in a Data Access Application
Data Access Application	The Central Platform shall store pre-selected Distributions in a 'basket', allowing them to be included later in a Data Access Application
Data Access Application	The Central Platform shall provide with a Data Access Application form to be filled by the data user.
Data Access Application	The Central Platform shall allow Data Access Application submissions by encoding the Data Access Application's form and selected EU dataset record distributions in a format allowing transmission via the HealthData@EU infrastructure.
Data Access Application	The Central Platform shall receive Status updates and Data Permits for Data Access Applications via eDelivery *
Data Access Application	The Central Platform shall provide with a Status update on the submitted Data Access Applications.
Catalogue Dataset Record Repository	The Central Platform shall accept Health DCAT-AP metadata to be created, read, updated, and deleted via RESTful APIs.
Catalogue Dataset Record Repository	The Central Platform shall expose its RESTful APIs for Metadata create, read, update, and delete via eDelivery to be accessible from the national nodes.
Catalogue Dataset Record Repository	The Central Platform shall perform validation on the create, update, delete requests for validity and structural integrity, and respond with success or error messages accordingly.

Level	Requirement
Catalogue Dataset Record Repository	The Central Platform must provide a mechanism to track all updates of metadata descriptions and maintain change history.
Data Upload	The Central Platform shall store files referenced by a URL in the Health DCAT-AP Metadata
Data Upload	The Central Platform shall provide with APIs for retrieval of stored files

10.3 Annex 3 ITB Use Case 3.0 - Validate Conformance with the HealthData@EU Infrastructure

Description:

The Interoperability Test Bed (ITB) is a service provided by the Directorate-General for Digital Services (DIGIT) of the European Commission. It supports the conformance testing of IT systems, playing a vital role in ensuring seamless communication and mutual understanding between systems through the exchange of messages. The ITB is employed for activities such as onboarding, establishing connectivity, and verifying conformance.

Actor(s):

The actors is this use case are Community Administrator or Member State user

Basic flow 1: Validate connectivity

- Description:
  This flow describes how the user can test and validate the connectivity of a National Contact Point (NCP), according to defined standards and protocols, with the HealthData@EU Central Platform Infrastructure via Domibus.
- Preconditions:
  The user is logged in to ITB
  The new National Contact Point has been onboarded to the HealthData@EU Infrastructure.
- Steps:

1. The user selects the required Member State from the ITB interface.
2. The system displays the Member state details page containing:
   .a The technical Domibus details of the National Contact Point
   .b The system tests, the user can perform through the interface
   .c The logged in user details
   .d The REST API keys of the system tests available
3. The user selects the HealthData@EU Connectivity system tests.
4. The system displays the specification defined for the ITB system test selected.
5. The user selects the specification they need to validate.
6. The system displays the “Conformance statement details” page, that consists of:

.a The specification description
.b The associated Connectivity tests available for performing the test selected and its execution steps.
.c Details about the test execution status.

7. The user can then proceed with running the test needed.
8. The system displays the progress of the steps executed and their outcome. A corresponding test report is created and can be downloaded.

- Post conditions:
  The user successfully performed connection validation with the HealthData@EU Infrastructure.

10.4 Annex 4 - Methodology

This Milestone has been drafted through four successive phases, each designed to keep the text faithful to two authoritative sources: the EHDS regulation (primarily Chapter V on the common IT infrastructure) and the "HealthData@EU - Architecture Model & Technical Specification (Release 4)".

Phase 1 - Scoping and gap analysis:
The editorial team began with internal framing sessions to clarify the exact policy-level objective of the document. Using a simple comparison grid, every paragraph of the Release 3 (later Release 4) technical specification relevant to cross-border connectivity was matched against Articles 36 and 75 of the regulation. This exercise highlighted missing explanations and terminology mismatches; those items formed the gap-analysis register that guided the rest of the work.

Phase 2 - Detailed outline:
Findings from the gap analysis were reviewed in "chamber" sessions then we proceed to 2 virtual workshops with all named contributors. Together, the group agreed on the chapter headings, the order in which they should appear and the legal cross-references to be cited in each. Section ownership was allocated at the end of this phase.

Phase 3 - Collaborative drafting:
Writing moved to short "write-in-chambre" sprints. During each sprint, authors worked on their assigned section, autonomously, and offline. A rolling editorial review ensured that the narrative followed the TEHDAS Handbook template and that every statement could be traced back to the regulation or the technical specification.

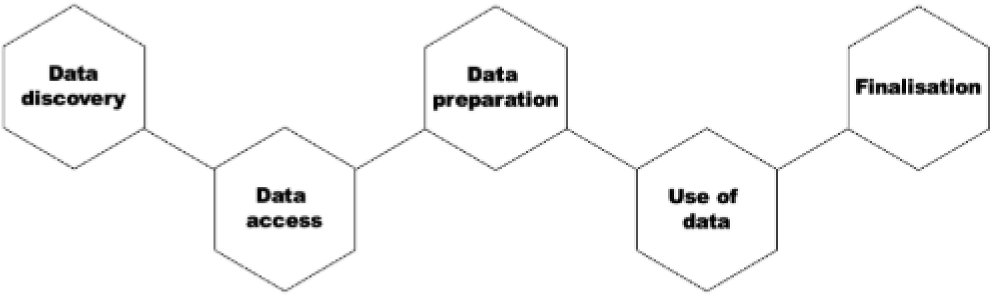
Phase 4 - Consolidation:
Once a complete draft was assembled, it circulated among contributors for comment. Feedback was incorporated in a single pass, and an Open Questions list was created to capture issues that will require input during the forthcoming public consultation.

10.5 Annex 5 - User journey

User journey

When a data user[1] applies for electronic health data for secondary use purposes, such as research and innovation activities, education, and policymaking, 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 form to a health data access body (HDAB)[2]. 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 applicant seeks to use individual-level data.

Data request form is used when the applicant wants to apply for aggregated (non-individual-level) data.

Data preparation

[1] Data user = a person using electronic health data for a secondary use purpose

[2] Health data access body (HDAB) = the authority responsible for assessing the information provided by the data user who applies for electronic health data for a secondary use purpose

During this phase, the data holder(s)[3] 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 environment4. 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.

[3] Data holder = Any natural or legal person, public authority or other body in the healthcare or the care sectors that has the right or obligation to provide electronic health data for secondary use purposes or the ability to make such data available (see more EHDS regulation Art. 2 (1t))

[4] Secure processing environment = an environment with strong technical and security safeguards in which the data user can process personal level electronic health data

10.6 Annex 6 - Glossary

Term	Definition
Access permit	Machine-actionable data structure that contains the information from data permit in a standardised format that can be securely transferred and acted on by computer services
Access point	A component of the HealthData@EU infrastructure that ensures secure, point-to-point message exchange between National Contact Points and the central platform. Access Points exist at both the national and EU levels and enable the technical interconnection required by Articles 36(3d) and 75 of the Regulation.
Additional information (related to pseudonymisation)	Additional information is information whose use enables the attribution of **pseudonymised data** to identified or identifiable persons (EDPB Guideline 01/2025 Glossary, version adopted for public consultation). This term is specific to **pseudonymisation** and related to the "additional information" referred to in Regulation (EU) 2016/679 Article 4(5) (GDPR).
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)
Anonymisation metadata	Anonymisation metadata refers to a structured set of detailed information describing (a) the methods and parameters used to anonymise a dataset, and (b) the resulting **quality metrics** used to anonymise a dataset or data processing result, or to assess their anonymisation. It includes details e.g., on applied techniques and transformation logs. This metadata helps assess data protection, track modifications, and ensure compliance with anonymisation criteria.
Anonymisation result	The output of anonymisation, which can be an anonymised dataset or a data processing result including **anonymisation metadata**.

Term	Definition
Anonymised statistical format	An anonymised statistical format refers to aggregated data that does not include information on individual data subjects or entities, also labelled as non-personal aggregated data.
Attribution of pseudonymised data to data subjects	Process that establishes that **pseudonymised data** relate to an already identified person, or links the data to other information with reference to which the data subjects could be identified. (EDPB Guideline 01/2025 Glossary, version adopted for public consultation)
Authorised user	An authorised natural person listed in the data permit, giving them the rights to process sensitive data inside an SPE
Benefits (of data use)	Refers broadly to positive outcomes of data use. It can encompass social, health and environmental aspects, among others.
Central Platform	An interoperability platform established by the European Commission, providing services to support and facilitate the exchange of information between National Contact Points and authorised participants in HealthData@EU for secondary use of electronic health data. (EHDS Regulation, Article 75(8))
Consistent pseudonymisation	Two sets of data are considered to be pseudonymised consistently if data contained in those sets and relating to the same person can be linked on the basis of the **pseudonyms** they contain (EDPB Guideline 01/2025 Glossary, version adopted for public consultation). Consistency is context-specific and may be limited to a **pseudonymisation domain**.
Cross-border gateway	Handles the transmission and reception of communications between one National Contact Point and Central Services in a secure and technically standardised manner. It supports the eDelivery protocol (HD@EU Pilot WP5 – Architecture Definition).
Data access	Processing by a data user of data that has been provided by a data holder, in accordance with specific technical, legal, or organisational requirements, without necessarily implying the transmission or downloading of such data. (DGA, Article 2(8)(9)(13))

Term	Definition
Data aggregation	A process by which information is collected, manipulated and expressed in summary form (ISO/TR 12300:2014(en), 2.1.4)
Data anonymisation framework	A set of processes and practices designed to ensure data privacy through anonymisation and **privacy risk assessment**.
Data combination	The process of bringing together data from multiple datasets that can be processed pursuant to one or multiple data permit(s) or data request(s) (Regulation (EU) 2015/327 (EHDS) Articles 57, 68, 69) or other legal basis (such as consent or permits based on other legislation than EHDS). Data linkage can be part of this process.
Data consolidation	A process of combining data from multiple sources, cleaning and verifying them, removing errors so that they can be prepared for provision. Data consolidation may include creation of data subsets, data extraction, duplicates elimination, quality control and data linkage aspects.
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.

Term	Definition
Data holder application (a software linked to the Secure Processing Environment)	A software application that provides the data holder with secure digital access to the Secure Processing Environment (SPE). Its core functions include facilitating the upload and download of data in accordance with the data holder's responsibilities under the EHDS regulation.
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 to only collect, store and process personal data in a manner that is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. (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 EHDS Regulation. (EHDS Regulation, Article 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,

Term	Definition
	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 processing result	Data processing result refers to outputs from data processing activities carried out by the health data user. It may be generated from statistical analysis or machine learning algorithms, including descriptive statistics, model coefficients, performance indicators, visualisations.
Data processor	The data processor should handle data exclusively in the manner prescribed by the controller. A data processor acts under the detailed instructions of the data controller only, by processing personal data on their behalf. (GDPR, Article 4(1)(8))
Data protection	The "implementation of appropriate administrative, technical or physical means to guard against unauthorized intentional or accidental disclosure, modification, or destruction of data (ISO/IEC 20944-1:2013(en), 3.6.5.1).
Data provenance	Data provenance means a **description of the source** of the data, including context, purpose, method and technology of data generation, documenting agents involved in the provenance of data, data validation routines, source data verification, traceability of changes, and quality control of data.
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(2z))
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(2aa))

Term	Definition
Data user application (a software linked to the Secure Processing Environment)	A software application that provides the data user with secure, computerised access to their workspace within the Secure Processing Environment. Its primary functions include facilitating the upload and download of data while ensuring robust authentication and authorisation mechanisms to prevent unauthorised access.
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(2y))
Dataset record	A dataset record is a single, structured unit of data within a dataset, analogous to a row in a table or a record in a database. It contains specific information about a single entity or instance within the broader dataset.
Dataset subset	Dataset subset contains only selected records, variables or elements from a larger dataset while maintaining its key characteristics and relationships.
Dataset description	Health data access bodies shall, through a publicly available and standardised machine-readable dataset catalogue, provide a description in the form of metadata of the available datasets and their characteristics (EHDS Article (77(1))
Direct identifier	A data element (or set thereof) that has been assigned or is being used to distinguish the data subject it refers to from all others in the given context without requiring the use of **additional information**. Examples are passport or social security number, or the set consisting of first and last name as well as date of birth. (EDPB Guideline 01/2025 Glossary, version adopted for public consultation)

Term	Definition
Disclosure control	Disclosure control refers to techniques and procedures applied to datasets to reduce the privacy risks for individuals when the data is disclosed to data users.
Dispatcher	A component of the HealthData@EU infrastructure that enables the secure transmission, routing and delivery of structured electronic messages (such as dataset records and access requests) between national and central systems.
Electronic health data	Personal or non-personal electronic health data (EHDS Article 2(2c)).
EU dataset catalogue	A dataset catalogue means 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 Regulation, Article 2(2y)) The EU dataset catalogue, the national dataset catalogues and the dataset catalogues of authorised participants in HealthData@EU shall be made publicly available. (EHDS Regulation, Article 79(1–2))
Federated analysis	A decentralised approach to data analysis where statistical results are computed locally on distributed data resources rather than aggregating raw data centrally. This method enables benchmarking, multi-site research, and collaborative analytics while preserving data privacy and security. Only aggregated insights or summary statistics are shared between nodes, ensuring compliance with data protection regulations.
Federated learning	A decentralised machine learning approach where models are trained and validated on distributed data resources without transferring raw data. Instead, only model updates or gradients are exchanged between nodes, enhancing data privacy and security. This method enables collaborative model development across multiple organisations or devices while maintaining local data sovereignty and regulatory compliance.

Term	Definition
Federated processing	A decentralised data processing approach where computations occur locally on distributed nodes rather than being centralised. This method enables data to remain on local devices or servers while only aggregated results or model updates are shared, enhancing privacy and security. It is commonly used in machine learning (“federated learning”), analytics (“federated analysis”), and secure data collaborations across multiple organisations.
Fidelity	Fidelity (or resemblance**)** refers to the extent to which processed data—such as anonymised data—retains the statistical properties, relationships, and structural characteristics of the **original data**. High fidelity means that distributions, correlations, and key patterns remain intact.
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 (HDAB)	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, HDABs are required to publicly list information on the data permits issued. (EHDS Article 55 and Recital 52)
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 Regulation.
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

Term	Definition
	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(2t))
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 Regulation, Article 2(2u))
High Performance Computing (HPC)	HPC is the use of advanced and not commonly available computational infrastructure – such as supercomputers or compute clusters – to solve highly complex and resource intensive computational problems.
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

Term	Definition
	as an intel lectual 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	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)
Interoperability	Ability of organisations, as well as of software applications or devices from the same manufacturer or different manufacturers, to interact through the processes they support, involving the exchange of information and knowledge, without changing the content of the data, between those organisations, software applications or devices. (EHDS Regulation, Article 2(2f))
Irreversible pseudonymisation	A pseudonymisation method where the **pseudonymising transformation** cannot be reversed. The information necessary to re-establish the link between the **pseudonym** and the **original data** has been permanently destroyed or is otherwise unavailable.
Legal basis of data processing	The conditions under which personal data processing is considered lawful (GDPR, Article 6). Purposes for which the electronic health data can be processed for secondary use are laid down in EHDS Regulation, Article 53.
Metadata	A structured description of the contents or the use of data facilitating the discovery or use of that data. (Data Act, Article 2)
National contact point (NCP)	A National Contact Point for secondary use is the organisational and technical gateway for making electronic health data available for secondary purposes, including research, innovation, policy-

Term	Definition
	making, and public health. It plays a crucial role in connecting national data infrastructures to the HealthData@EU Central Platform, enabling secure and efficient data sharing across borders. (EHDS Regulation, Article 75(1))
Non-compliance	Any failure to comply with any requirement under the Union harmonisation legislation.
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))
Observational Medical Outcomes Partnership (OMOP) common data model (CDM)	A standardised, common data model (CDM) specification originally developed by the Observational Medical Outcomes Partnership (OMOP) and now maintained by the Observational Health Data Sciences and Informatics (OHDSI) community. It defines a consistent structure and a set of standardised vocabularies for observational health data, enabling researchers to perform large-scale, reproducible analyses across diverse databases.
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 Open Data Directive)
Open (data) database	Publicly accessible digital data that anyone can freely use, reuse, and redistribute for any purpose.
Original data	Individual-level health data prior to any application of **pseudonymisation, anonymisation**, or **synthetic data generation**. It consists of raw data that directly represent real-world individuals.

Term	Definition
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))
Privacy (of synthetic or anonymised data)	Privacy measures the extent to which anonymised or synthetic data protects individuals from re-identification, membership inference, or sensitive information leakage. High privacy ensures that no single individual can be traced back to the real dataset, nor can their participation in the **dataset** be inferred.
Privacy risk assessment	Overall process of identifying, analysing, evaluating, consulting, communicating and planning the treatment of potential privacy impacts with regard to the processing of personally identifiable information (3.7), framed within an organisation's broader risk management framework (ISO/IEC 29100:2024(en), 3.18). **Re-identification risk assessment** falls under privacy risk assessment, together with attribute inference and group membership, for example.
Pseudonym	Identifier that is added to data during the **pseudonymising transformation** and set in such a way that it can be attributed to data subjects only using **additional information**. (EDPB Guideline 01/2025 Glossary, version adopted for public consultation)
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))
Pseudonymisation domain	Environment in which the controller or processor wishes to preclude attribution of data to specific data subjects. May incorporate persons acting under the authority of the controller or processor, respectively, other natural or legal persons, public authorities, agencies or other bodies, and their respective technological and informational resources. Does not include persons authorised to process additional data allowing the attribution of the **pseudonymised data** to data

Term	Definition
	subjects. (EDPB Guideline 01/2025 Glossary, version adopted for public consultation)
Pseudonymisation entity	The entity responsible of processing identifiers into pseudonyms using the pseudonymisation function. It can be a data controller, a data processor (performing pseudonymisation on behalf of a controller), a **trusted third party** or a data subject, depending on the pseudonymisation scenario. It should be stressed that, following this definition, the role of the pseudonymisation entity is strictly relevant to the practical implementation of pseudonymisation under a specific scenario. (ENISA, Pseudonymisation techniques and best practices, p. 10)
Pseudonymisation secrets	Data that is used in the application of the **pseudonymising transformation** or is created during that process, for example cryptographic keys or salts, and allows the computation of pseudonyms from certain identifying attributes. Part of **additional information**. (EDPB Guideline 01/2025 Glossary, version adopted for public consultation)
Pseudonymised data	Result of applying the **pseudonymising transformation** to some personal data. Cannot be attributed to a specific data subject without **additional information**. (EDPB Guideline 01/2025 Glossary, version adopted for public consultation)
Pseudonymising controller or processor	Controller or processor that uses pseudonymisation as a safeguard and modifies **original data** according to Regulation (EU) 2016/679 (GDPR) Article 4(5). (EDPB Guideline 01/2025 Glossary, version adopted for public consultation)
Pseudonymising transformation	Procedure that modifies **original data** in a way that the result cannot be attributed to a specific data subject without **additional information**. (EDPB Guideline 01/2025 Glossary, version adopted for public consultation)
Public use file	A **dataset** made available to the public, typically containing anonymised, synthetic or aggregated data to protect individual privacy. These files can be released to data users for information and testing purposes

Term	Definition
	before they apply for a data permit. It is based on **original data**.
Public value (of data use)	Public value means a weighted composite of risks and benefits of the data use taking into account the sustainability of benefits, addressing future societal needs, distributing benefits fairly, evaluating potential harm, ensuring stable safeguards through risk assessment, and correcting any harms that may occur.
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).
Quality metrics	Quality metrics refer to qualitative and quantitative indicators used to assess the fitness for purpose of a dataset. In the context of synthetic and anonymised data, quality metrics are particularly relevant to evaluate how transformations affect the data's **utility**, **fidelity**, and **privacy**. Quality metrics may also be used to assess pseudonymised or original datasets, particularly when serving as a benchmark or when evaluating fitness for specific secondary use purposes. (Adapted from ISO and EHDS principles; EHDS Regulation, Article 66 and Recital 58)
Quality metrics evaluation	Quality metrics evaluation refers to the calculation or derivation of the **quality metrics**.
Quality metrics tool	Quality metrics tool (or "metrics tool") refers to a software, an algorithm, a processing pipeline, a documented manual process, or a combination of these, designed to perform **quality metrics evaluation**.
Quasi-identifier	A **dataset** attribute that, when considered in conjunction with other attributes are sufficient to attribute at least part of the pseudonymised data to data subjects. (EDPB Guideline 01/2025 Glossary, version adopted for public consultation)

Term	Definition
Re-identification	The process of associating data in a de-identified **dataset** with the original data principal (i.e., data subject) (ISO/IEC 20889:2018(en), 3.31).
Re-identification risk	The risk of a successful re-identification attack (ISO/IEC 20889:2018(en), 3.33), which describes an action performed on de-identified data by an attacker with the purpose of **re-identification** (ISO/IEC 20889:2018(en), 3.32).
Representational State Transfer Application Programming Interface (RESTful API)	An application programming interface used for building scalable and interoperable web services. RESTful API follows the principles of Representational State Transfer (REST), using standard HTTP methods to perform operations on resources identified by URLs. It emphasises stateless interactions, meaning each request contains all necessary information without relying on server-side sessions.
Reversible pseudonymisation	The **pseudonymisation entity** uses a **pseudonymising transformation** process that allows the pseudonymisation entity to reverse the **pseudonym**, if necessary. For example, by using separately kept matching tables of pseudonyms and identifying data, or computable secrets allowing for calculating back to the original input.
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)

Term	Definition
Sensitive data	Data with potentially harmful effects in the event of disclosure (i.e., providing access to data to a third party) or misuse (ISO 5127:2017(en), 3.1.10.16)).
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.
Synthetic data documentation	Documentation of a synthetic dataset generated automatically or semi-automatically by the **synthetic data generator**. The documentation shall be anonymised so that it can be accompanied with the synthetic data set when released for the data user or for public use.
Synthetic data generator	A synthetic data generator is a software application, model or algorithm designed to generate **synthetic data**. It uses real-world data as input and generates a synthetic dataset. It is also possible to use parameters derived from the **original data** as input and/or modify additional parameters entered by the user.
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

Term	Definition
	keep it secret. (Trade Secret Directive (2016/943), Article 2(1))
Transfer of data outside the EU/EEA	General principles, adequacy decisions, appropriate safeguards and specific derogations for transferring personal data to third countries or international organisations (GDPR, Chapter 5, Articles 44–50). The European Data Protection Board (EDPB) identifies three cumulative criteria to identify a transfer outside the EEA: • ”a controller or a processor is subject to the GDPR for the given processing; • this controller or processor discloses by transmission or otherwise makes personal data available to another organisation (controller or processor); • this other organisation is in a country outside EEA or is an international organisation.”
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 Regulation, Article 72 and Recital 76)
Trusted Research Environment (TRE)	TREs emerged from the UK health research sector, shaped by community-led principles and structured around flexible, function-based zones. They aim to create trusted, auditable access to sensitive data, often under national governance frameworks. TREs are not the same as Secure Processing Environments, which are legally defined in the EHDS Regulation.
Trusted third party (TTP)	A **pseudonymisation entity** which is independent from the data user and data holder that processes identifiers into pseudonyms. (ENISA, Pseudonymisation techniques and best practices). The TTP needs only to

Term	Definition
	know the identifiers of the data subjects on the basis of which it will compute the **pseudonyms**, and no other data. (EDPB Guideline 01/2025 Glossary, version adopted for public consultation)
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.
Request for payment	A formal request submitted to the data user for payment of the actual costs corresponding to work completed during a specific period. It follows the structure defined in the original invoice and refers to the relevant cost components outlined therein.
Payment instalment	One of several scheduled payments made in response to requests for payment. Each instalment corresponds to a portion of the total cost, aligned with the progress of the procedure or delivery of services.
Payment	The financial transaction by which the user transfers the requested amount to the Health Data Access Body, Trusted Data Holder or the Data Holder in response to a request for payment.
Utility	Utility refers to how well the data supports its intended use, such as syntactical testing, analytical tasks, decision-making, or machine learning model performance. In the context of anonymised and synthetic data high utility means that insights, predictions, or outcomes derived from the data closely match those obtained using the **original data**.