D6.4 Technical Specifications for Data Access Application Management System (DAAMS) for Health Data Access Bodies (HDABs)

TEHDAS2 – Second Joint Action Towards the European Health Data Space

17 September 2025

Co-funded by the European Union

0 Document info

0.1 Authors

Author(s)	organisation
Radovan Tomasik	Ministry of Health, Czech Republic
Pinar Alper	Luxembourg National Data Service
Azul O'Flatery	Department of Health, Ireland
Sam Santosh	Maynooth University, Ireland
Ana Martin-Moreno	Ministry Of Health of Spain, Spain
Zdenek Gütter	Ministry of Health of the Czech Republic
Ana Muzinic	Federal Institute for Drugs and Medical Devices, Germany
Karel Winderickx	Belgian Health Data Agency, Belgium

0.2 Keywords

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

0.3 Document history

Date	Version	Editor	Change	Status
05.09.2025	0.4	Radovan Tomasik	Internal Review	DRAFT
30.06.2025	0.3	Radovan Tomasik		DRAFT
26.05.2025	0.2	Radovan Tomasik		DRAFT
13.11.2024	0.1	Radovan Tomasik		DRAFT

Table of Contents

1 List of abbreviations

Name	Abbreviation
Application Programming Interface	API
Community of Practice	CoP
Data Catalogue Vocabulary Application Profile	DCAT-AP
Data Governance Act	DGA
Directorate-General	DG
European Health Data Space	EHDS
European Union	EU
General Data Protection Regulation	GDPR
Geospatial Data Catalogue Application Profile	GeoDCAT-AP
Graphical User Interface	GUI
Health Data Access Body	HDAB
Health Data Catalogue Vocabulary Application Profile	HealthDCAT-AP
Joint Action	JA
Minimum Viable Product	MVP
National Contact Point	NCP
Statistical Data Catalogue Vocabulary Application Profile	StatDCAT-AP
The Finnish Innovation Fund	Sitra
Towards the European Health Data Space	TEHDAS
Second Joint Action Towards the European Health Data Space	TEHDAS2
Work Package	WP
HealthData@EU Central Platform	CP

2 Executive summary

The Data Access Application Management System (DAAMS) is a national platform designed to enable secure and compliant access to electronic health data for secondary usage across the European Union, in alignment with the European Health Data Space (EHDS) regulation. Its primary role is to support the handling of both health data access applications and health data requests for secondary uses purposes, such as research, innovation, policymaking and other purposes listed in *Art. 53 EHDS*.

DAAMS is operated by Health Data Access Bodies (HDABs) at national level. It manages the full application lifecycle and interacts with both national applicants and the cross-border EHDS infrastructure (via the National Contact Point).

This document provides the technical specifications required for Health Data Access Bodies (HDABs) in the European Union to develop and deploy a DAAMS. It includes functional and non-functional requirements, data models, process flows / business logic, and use cases. Any elements not explicitly defined here may be adapted to the national context, provided that they remain in compliance with the EHDS Regulation and support interoperability with the EHDS infrastructure.

3 Requirement terms definition

The following terms, as defined in **RFC 2119**, are used to specify the strictness of various requirements and recommendations in this document:

1. **MUST**: This word, or the terms "REQUIRED" or "SHALL", means that the definition is an absolute requirement of the specification. In the context of DAAMS, when something is described as "MUST," it means that the system must comply with the specific technical or security requirement. For example, "The system MUST use encryption for data in transit."

2. **MUST NOT**: This phrase means that the specification defines something as being absolutely prohibited. When DAAMS documentation states that something "MUST NOT" occur, it is forbidden for reasons of security, privacy, or compliance. For instance, "Health data MUST NOT be accessed without proper authentication."

3. **SHOULD**: This term, or the adjective "RECOMMENDED", means that there may be valid reasons in some cases to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course. In DAAMS, when something is described as "SHOULD," it is highly advised but not strictly mandatory. For example, "The system SHOULD support multi-factor authentication to enhance security."

4. **SHOULD NOT**: This phrase means that there may exist valid reasons in some cases where a particular behaviour is acceptable or even useful, but the full implications should be understood, and the case carefully weighed before implementing any action described with "SHOULD NOT". For example, "Data from wellness applications SHOULD NOT be processed unless specifically required for secondary use."

5. **MAY**: This word, or the adjective "OPTIONAL", means that the item is truly optional. One vendor may choose to include the item because it enhances functionality, while another may omit it. In DAAMS, "MAY" is used to specify features or behaviours that are optional. For example, "The system MAY provide users with personalized notifications on data access events."

4 Terminology Definition

IMPORTANT NOTE TO READERS: The terminology definitions in this section are a normative portion of this specification, imposing requirements upon implementations. All the capitalized words in the text of this specification, such as "Data Permit", reference these defined terms. Whenever the reader encounters them, their definitions found in this section must be followed. For more context to these terms see the EHDS Regulation.

5 Introduction

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, 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 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: 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.

5.1 Purpose of this document

The purpose of this specification document is to define the technical and functional requirements for the development and operation of the Data Access Application Management System (DAAMS) in accordance with the European Health Data Space (EHDS) Regulation.

DAAMS serves as a national platform managed by Health Data Access Bodies (HDABs) to facilitate secure, transparent, and standardised access to electronic health data for secondary use. This document aims to provide Member States with a common specification for implementing DAAMS, ensuring interoperability across the European Union while allowing flexibility for national adaptation.

The goals of the specification are to:

- Define functional and non-functional requirements for DAAMS, including core services such as application submission, evaluation support, status tracking, and permit lifecycle management
- Ensure compliance with EHDS Regulation, particularly regarding legal bases for data processing, data subject rights, and procedural safeguards;
- Enable interoperability with EU-level infrastructure, including HealthData@EU and secure processing environments, through clearly defined APIs and integration patterns;
- Support transparency and accountability by specifying mechanisms for audit logging, access control, and user notification;
- Provide a foundation for consistent user experience, both for applicants requesting data access and for HDABs reviewing requests;
- Allow for national customisation, enabling each Member State to extend or adapt the system in accordance with its legal and organisational frameworks, while maintaining compliance with shared EU-level standards.

5.2 Overview

DAAMS operates as a core component of the national portal for the European Health Data Space (EHDS), as established under Regulation (EU) 2025/327. While the term *national EHDS portal* can encompass the full range of IT services offered by a Health Data Access

Body (HDAB), this specification focuses on the DAAMS component responsible for the submission and processing of data access applications and data requests.

Specifically, DAAMS supports two main functions:

- Submission and management of national data access applications and data requests originating within the Member State;
- Reception and processing of data access applications and data requests submitted via the HealthData@EU Central Platform.

Figure 4 illustrates a high-level example of a national EHDS infrastructure, demonstrating how services such as DAAMS may be implemented as standalone components interoperating with other national systems via APIs. This modular approach supports flexibility in system design while ensuring compliance with the interoperability requirements defined by the EHDS Regulation (notably Chapter IV, and Articles 50–54).

This example assumes a simplified case where a single HDAB operates a single DAAMS within the national EHDS node. However, the regulation allows Member States to designate multiple HDABs (Article 51(3)), each potentially operating its own DAAMS instance. In such configurations, a coordinating HDAB (or the NCP) is expected to take responsibility for receiving applications (which are always received via the NCP) and distributing them to the appropriate HDAB and DAAMS instance within the Member State.

This specification supports both single and multi-DAAMS models, with the aim of ensuring consistent cross-border interoperability regardless of internal national structure.

Implementations of DAAMSs MAY take use of open-source components developed by the European Commission available on code.europa.eu.

5.3 Scope

This specification document defines the functionalities, interfaces and integration requirements necessary to ensure functional and standardized Data Access Application Management Systems compatible with the HealthData@EU Central Platform, as outlined in the EHDS Regulation. It focuses on the standardised components required to support the exchange of data access application, data request and decision related information across Member States and the entire federated EHDS IT infrastructure.

The scope of this document is deliberately limited to those aspects of DAAMS that MUST be harmonised at the European level in order to guarantee interoperability. While adhering to this constraint, the document also lists suggestions and recommendations promoting further standardization and sustainability. Member States retain full autonomy in how they design, implement, and operate their national DAAMS systems, including the choice of technologies, data models and internal processes. However, to maintain regulatory compliance, these systems must be capable of interfacing with the HealthData@EU Central Platform and other cross-border services via the common, standardised protocols and data exchange formats defined in this specification.

This specification includes:

- **Mandatory technical requirements** for the connection between national systems and the central platform;
- **Guidance on integration patterns** to support a range of national deployment models;
- **Recommended practices and design choices** to enhance interoperability, reusability, and maintainability of DAAMS components across the EU;
- **Specifications for information exchange**, covering key events such as application submission, status updates, permit issuance, and audit logging where applicable.

Out of scope are national-level implementation details, internal decision-making processes of Health Data Access Bodies, and the operation of secure processing environments. Other examples of out-of-scope peripheral functions are Opt-out Management, Helpdesk, Fees and invoicing Management. These and other not mentioned aspects are left to national discretion, provided regulatory compliance and that the interoperability interface to the EU infrastructure is respected.

DAAMS, as a component of the national EHDS infrastructure, may be implemented as part of the same system as the National Health Dataset Catalogue; however, this is not a strict requirement. The handover of selected datasets from the catalogue to DAAMS—for the purpose of initiating a new data access application or request—can be facilitated via a defined API, enabling a modular architecture with clear separation of concerns.

Given that national implementations may involve the integration of multiple systems, the decision to adopt a monolithic or modular architecture is left entirely to the implementers. If a modular architecture is chosen, special attention SHOULD be given to ensuring a unified user experience across components, particularly where multiple roles and systems interact within a single workflow.

6 Submitting Applications – DAAMS Front Office

DAAMS MUST provide a Graphical User Interface (GUI) web interface through which applicants can place national data access applications or data requests.

DAAMS GUI web interface MUST support at least one official language of the European Union, and, in addition, it SHOULD also support the English language.

DAAMS GUI web interface SHOULD allow the applicant to configure the language settings.

DAAMS MUST provide a user space for applicants for them to create draft application forms, submit applications and track application status.

DAAMS MUST provide respective templates/forms to allow applicants to create data access applications or data requests.

DAAMS MUST allow users to create a data access application or data request for one or more datasets described in the National Health Dataset Catalogue.

DAAMS MAY adopt the commonplace “shopping cart” metaphor to allow users to select multiple datasets prior to creating a data access application (or data request).

For each dataset included in a data access application (or data request) the DAAMS MUST display, in a read-only manner, descriptive information on the dataset and the associated HDABs that will be the recipient of the application.

The access application form provided by the DAAMS MUST match the information requirements of the EU Common Data Access Application form. These forms will be further specified by implementing acts adopted under Article 70(2) of the EHDS Regulation.

The access application form provided by the DAAMS MAY include additional information requirements deemed necessary by the HDABs, e.g. variable-level specification of scope of data delivery, study population and inclusion-/exclusion criteria.

The data request form provided by the DAAMS MUST match the information requirements of the EU Common Data Request form. These forms will be further specified by implementing acts adopted under Article 70(2) of the EHDS Regulation.

The data request form provided by the DAAMS MAY include additional information requirements deemed necessary by the HDABs, e.g. variable-level specification of scope of data delivery, study population and inclusion-/exclusion criteria.

DAAMS SHOULD guide the applicant in filling out the form by ordering the presentation of form fields in sections.

DAAMS MAY automatically populate fields concerning applicant information using applicant's login profile.

DAAMS MUST highlight mandatory form fields and display field guidance text to assist the applicants when filling in forms.

DAAMS MUST provide appropriate field validations functions and display validation errors to the applicant as messages.

DAAMS MUST allow applicants to save forms as draft (without submitting them) so that they can continue filling the form later.

DAAMS MUST allow applicants to modify a previously saved draft form.

DAAMS MAY allow the applicant to create a copy (or clone) of a draft form.

DAAMS SHOULD allow applicants to add additional datasets to a draft data access application (or data request) form.

DAAMS MUST NOT allow the submission of a form that is missing required fields or has field validation errors.

DAAMS SHOULD highlight to the applicant when all required fields (in all sections) of the form are complete, and all field validations are successful.

DAAMS MUST allow the applicant to submit an application.

DAAMS MUST allow the applicant to track status of their application(s), including at a minimum, the states identified in Section 7.2 of this specification.

DAAMS SHOULD highlight expected and actual timeframes for the statuses that an application can be in, thereby, DAAMS SHOULD display approaching deadlines and overdue tasks of applicants. e.g. Applicant will have 1 month to provide additional information on an application that has been sent back to them for completion by the HDAB.

DAAMS MUST enable the applicant to provide additional information on an application which they had submitted and the HDAB considers to be incomplete (EHDS Art. 68).

DAAMS SHOULD provide a messaging interface allowing exchanges between the applicant and HDAB assessor, while ensuring auditability and data protection.

DAAMS web interface MAY provide front end to the messaging interface via structured GUI elements e.g. tagged, field-level comments or system-generated requests for clarification, with audit trail.

For applications requiring additional information by the HDAB, the DAAMS MUST display to the applicant:

- the application ID,
- the form fields flagged by the HDAB as requiring further information and comments placed by the HDAB.

Per form field flagged by the HDAB, the DAAMS MUST allow the applicant to enter the required further information and save the form.

When the HDAB requests additional information from the applicant, the DAAMS MUST enable the applicant to provide the requested input by updating the relevant fields. This process does not constitute a formal re-submission of the application in the regulatory sense, but rather a continuation of the existing application process. The updated information MUST be recorded and transmitted to the HDAB, and the application status MUST reflect the progression (e.g. from "AWAITING_ADDITIONAL_INFORMATION" to "PROCESSING").

DAAMS MUST allow the applicant to withdraw a submitted application.

GUI web interface provided by the DAAMS SHOULD be compliant with Web Content Accessibility Guidelines (WCAG) version 2.0 or above. The interface SHOULD meet applicable requirements originating from the Web Accessibility Directive and Harmonised European Standard Harmonised on Accessibility.

DAAMS MUST allow applicant to view all draft forms in their user space.

DAAMS MUST allow applicants to cancel (or delete) a draft application form.

DAAMS MUST support HDAB-defined business rules regarding expiry of draft forms, e.g., a draft form not submitted within 6 months shall expire.

DAAMS MUST notify applicants when their draft forms will expire due to extended period of inactivity.

DAAMS MUST allow applicant to print draft and submitted forms.

DAAMS MUST allow export of submitted forms in a machine-actionable format.

DAAMS MAY allow populating draft forms by importing from a machine-actionable format.

DAAMS SHOULD allow the applicant to view all notifications targeted to the applicant ordered by their timestamps.

DAAMS MAY allow the applicant to search by free text over applications and notifications in their user space.

DAAMS MUST notify or show the applicant that fees will be charged from the moment an application is submitted and being evaluated.

7 Processing Applications- DAAMS Back Office

DAAMS is primarily responsible for processing national applications and those applications incoming from the HealthData@EU Central Platform. In the case of applications from the HealthData@EU Central Platform, DAAMS receives them via the NCP when a user submits them. DAAMS MUST NOT communicate directly with the HealthData@EU Central Platform.

At the link below, the HealthData@EU National Dispatcher OpenAPI specification can be found and interacted with. This API contains all the methods and schemas for the processing of applications in DAAMS:

National Dispatcher – OpenAPI Description

The same API will be available once the HealthData@EU National Dispatcher is deployed on the national infrastructure. The example below details how to configure the URL and access the same API on the national infrastructure.

Here is how to access it:
https://health-data-national-dispatcher.<localhostname>

An application has the following structure:
Message structure for a Data Access Application received by the NCP from the HealthData@EU Central Platform:

- Obtain the full list of received applications:
  `https://health-data-national-dispatcher.<localhostname>/#operation/getApplications`
- Obtain a single application using the application identifier:
  `https://health-data-national-dispatcher.<localhostname>/#operation/getApplication`

Data Access/Request Application	
HealthData@EU CP → NCP → DAAMS	
Attributes	**Description**
Title	Title given by the user to the Data Access/Request Application
Application_Type	Identification if its Data Access or Data Request application
Application ID	Unique identifier of the Data Access/Request Application on the HD@EU Central Platform
User	name of the user who submitted the Data Access/Request Application
Datasets	
Dataset_ID	Central identifier assigned to the Dataset that contains the distribution that was added to the Data Access/Request Application.
Title	Title of the Dataset
Country	Country of the Dataset

HDAB	Information about the HDAB that published the Dataset
Provenance	Provenance of the Dataset
Catalogue_ID	Central identifiers assigned to the Catalogue that holds the Dataset selected by the user.
Distributions	
Distribution_ID	Central Identifier of the distribution that was added to the application.
Distribution Title	Title of the selected distribution that was added to the application.
Date added	Timestamp of when the Data Access/Request Application was added
Form	Data Access\Request Application Form in the original laguage
Sections	List of sections contained on the Data Access/Request Application Form
Section Number	Identifier of the section
Fields - Values	Identifier of the field and their value
Country	Identification of the Country (applicable to section 6 only)
Form translations	
Language	Language of the application form after translation
Sections	List of sections contained on the Data Access/Request Application Form
Section Number	Identifier of the section
Fields - Values	Identifier of the field and their value
Country	Identification of the Country (applicable to section 6 only)
Attachments	Compressed zip file with the attachments submitted by the applicant on the various sections of an Application.

Message structure for an acknowledgement sent by DAAMS to the NCP after ingesting the previous message above:

Data Access/Request Application ACK	
DAAMS → NCP → HealthDATA@EU CP	
Attributes	**Description**
Application ID	unique identifier related to the acknowledged Data Access Application
StatusID	Central identifier of the Data Access Application status
Status Description	Description of the status
Date acknowledged	Timestamp of when the Data Access Application was acknowledged by DAAMS

DAAMS MUST allow access to the received data access application and data request only for authorized members.

DAAMS MUST be able to ingest applications submitted in any official language of the EU. Where the language differs from the national working language(s), the HDAB MAY request clarifications or translations, or may use translation tools as permitted under national procedures. Each application message MUST specify the application language.

7.1 Pre Screening - Data access applications

DAAMS MAY support a completeness check on data access applications to be conducted by HDAB personnel.

Where DAAMS is configured to include a completeness check:

> DAAMS SHOULD enable the outcome of the completeness check to be documented.
>
> DAAMS SHOULD enable applications deemed complete to proceed to assessment.
>
> DAAMS SHOULD enable the completeness check result to be stored as a structured entry in the application record and made available for audit.

TEHDAS guideline 6.3 makes recommendations on the steps that should be taken to conduct a completeness check.

Whether DAAMS is configured to include a completeness check or not:

> DAAMS MUST enable applications deemed incomplete by the HDAB to be returned to the applicant for completion; or to be rejected.
>
> DAAMS MUST enable HDAB personnel to document a structured justification for rejection as incomplete.

7.2 Pre Screening - Health Data Requests

DAAMS MUST enable HDAB personnel to conduct a completeness check of Health Data Requests.

TEHDAS guideline 6.3 makes recommendations on the steps that should be taken to conduct a completeness check.

DAAMS MUST enable HDAB personnel to document the outcome of the completeness check.

DAAMS MUST enable incomplete requests to be rejected by HDAB personnel.

DAAMS MUST enable HDAB personnel to document their justification for rejecting a request as incomplete.

DAAMS MUST enable complete requests to proceed to assessment.

7.3 Application assessment - Data Access Applications

DAAMS MUST enable HDAB personnel to document the outcome of their assessments of the application against the requirements set out in Article 68(1) (a)-(h). This must include providing justifications.

DAAMS MUST enable HDAB personnel to document the outcome of their assessment of the mitigation of risks referred to in Article 68(2). This must include providing justifications.

DAAMS MUST record the individual HDAB personnel member who conducted these assessments in part or in full.

Where HDAB decision making is supported by inputs from structures such as committees, DAAMS SHOULD enable storing these inputs and link them with the application.

DAAMS MUST enable HDAB personnel to document the decisions for each of the elements Article 68(10)(a)-(h).

DAAMS MUST enable storage of information shared by other HDABs or authorised participants in respect of applications from the HealthData@EU Central Platform.

DAAMS MUST enable the HDAB to record its overall assessment of the application including justifications.

DAAMS MUST enable the HDAB to record and store its formal decision on the application. This decision MUST be saved as a signed, time-stamped document (e.g. PDF) and linked to the application record.

In addition to the overall decision document, DAAMS MUST enable the structured storage of the individual elements listed under Article 68(10)(a)–(h), such as the permitted purposes, conditions of access, applicable safeguards, and data categories. These structured elements SHOULD be maintained in a format that facilitates future reporting and publication under Articles 58(1) and 57(1)(j) of the EHDS Regulation.

7.4 Application assessment - Health Data Requests

DAAMS MUST enable HDAB personnel to document the outcome of their assessment of the health data request. This must include providing justifications.

DAAMS MUST enable HDAB personnel to document their assessment of the mitigation of risks referred to in Article 68(2). This must include providing justifications.

DAAMS MUST enable the HDAB to record and store its formal decision on the data request. This decision MUST be saved as a signed, time-stamped document (e.g. PDF) and linked to the application record.

In addition to the overall decision document, DAAMS SHOULD enable structured storage of the delivery conditions associated with the data request decision, including anonymisation level, access method, applicable safeguards, and purpose. This supports future reuse in reporting and transparency under Articles 58(1) and 57(1)(j) of the EHDS Regulation.

7.5 Requesting additional information for a submitted application

DAAMS MUST enable HDAB personnel to request additional information from the applicant by marking specific fields in the submitted application. For applications from the HealthData@EU Central Platform, this request MUST be transmitted back to the HealthData@EU Central Platform via the NCP, using a structured message format. The request MUST include the application ID, the list of fields requiring clarification, and associated comments.

Upon receipt of the additional information, DAAMS MUST:

Update the status of the application to PRE_SCREENING

Notify relevant HDAB personnel

Acknowledge receipt via a message to the Central Platform

Message structure for a Data Access Application Additional Information Request sent by DAAMS to the NCP triggered by HDAB personnel:

https://health-data-national-dispatcher.< *localhostname* >/#operation/<requestInfo>

Data Access Application request for additional information	
DAAMS → NCP → HealthDATA@EU CP	
Attributes	**Description**
Application ID	Unique identifier of the Data Access Application on the HD@EU Central Platform
StatusID	Central identifier of the Data Access Application status
Status Description	Description of the status
Date	Timestamp of when the additional information was requested by DAAMS
Form	Data Access Application Form
Sections	List of sections contained on the Data Request Application Form
Section Number	Identifier of the section
Fields - Comments	Identifier of the field and comments
Country	Identification of the Country (applicable to section 6 only)

Message structure for a Data Request Additional Information Request sent by DAAMS to the NCP triggered by HDAB personnel:

Data Request request for additional information	
DAAMS → NCP → HealthDATA@EU CP	
Attributes	**Description**
Application ID	Unique identifier of the Data Request on the HD@EU Central Platform
StatusID	Central identifier of the Data Request status
Status Description	Description of the status
Date	Timestamp of when the additional information was requested by DAAMS
Form	Data Request Form
Sections	List of sections contained on the Data Request Form
Section Number	Identifier of the section
Fields - Comments	Identifier of the field and comments
Country	Identification of the Country (applicable to section 6 only)

7.5.1 Receiving additional information for a submitted application

DAAMS MUST be able to receive the additional information provided by the applicant upon request by an HDAB. It also MUST send a notification to the applicant that the updated application form was accepted and is being processed by HDAB.

Obtain the full list of received applications:

https://health-data-national-dispatcher.<localhostname>/#operation/getApplications

Obtain a single application using the application identifier:

https://health-data-national-dispatcher.< *localhostname* >/#operation/getApplication

Additional Information	
HealthData@EU CP → NCP → DAAMS	
Attributes	**Description**
Application ID	Unique identifier of the Data Request Application on the HD@EU Central Platform
User	name of the user who submitted the Application
Title	Title given by the user to the Data Request Application
Date submitted	Timestamp of when the Data Request Application was submitted
Form	
Sections	List of sections contained on the Data Access Application Form
Section Number	Identifier of the section
Fields – Values	Identifier of the field and its value
Country	Identification of the Country (applicable to section 6 only)
Form translations	

Sections	List of sections contained on the Data Access Application Form
Section Number	Identifier of the section
Fields – Values	Identifier of the field and its value
Country	Identification of the Country (applicable to section 6 only)

The following is a structure of an update acknowledgment message:

Additional Information ACK	
DAAMS → NCP → HealthDATA@EU CP	
Attributes	**Description**
Application ID	Unique identifier of the Application on the HD@EU Central Platform
Date received	Timestamp of when the updated Application was acknowledged by DAAMS.

7.6 Updating the status of Data Access Application

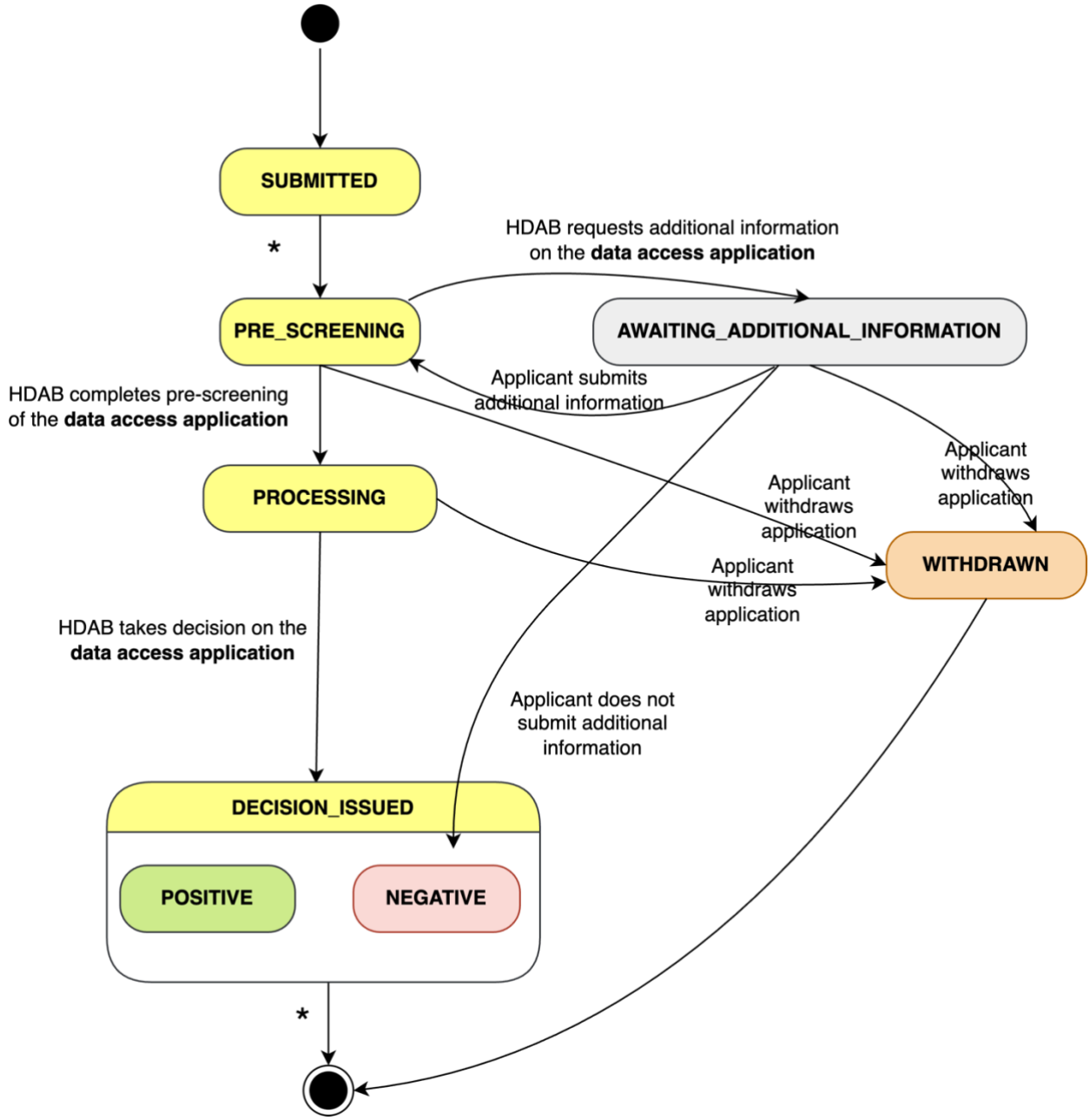
DAAMS MUST allow authorized HDAB personnel to update the status of received data access applications. The statuses listed below are those that MUST be supported for applications originating from the HealthData@EU Central Platform.

For Data Access Applications the following statuses are supported:

STATUS VALUE	Human readable label	Description
SUBMITTED	Submitted	An application of type data access application has been submitted and has been received by a DAAMS.
PRE_SCREENING	Pre screening	The application is undergoing a pre screening
PROCESSING	Processing	The application has been seen by HDAB personnel and is being assessed.
AWAITING_ADDITIONAL_INFORMATION	Awaiting additional information requested by the HDAB	HDAB has marked the application as incomplete, and the health data applicant must provide necessary information

DECISION_ISSUED	Decision has been issued	A decision for the access application has been made.
WITHDRAWN	Withdrawn	An application has been withdrawn

Figure 1 Data Acess Application State Machine Diagram



For data access applications from the HealthData@EU Central Platform DAAMS MUST send the following information to the NCP:

https://health-data-national-dispatcher.< *localhostname* >/#operation/<changeStatus>

Data Access Application Status Update	
DAAMS → NCP → HealthDATA@EU CP	
Attributes	**Description**
Application ID	unique identifier of the data access application
Status	Updated status value of the data access application

When the applicant has decided to withdraw their application, DAAMS will receive the following message:

Data Access Application Withdrawal	
HealthDATA@EU CP →NCP → DAAMS	
Attributes	**Description**
Application ID	unique identifier related to the acknowledged Application

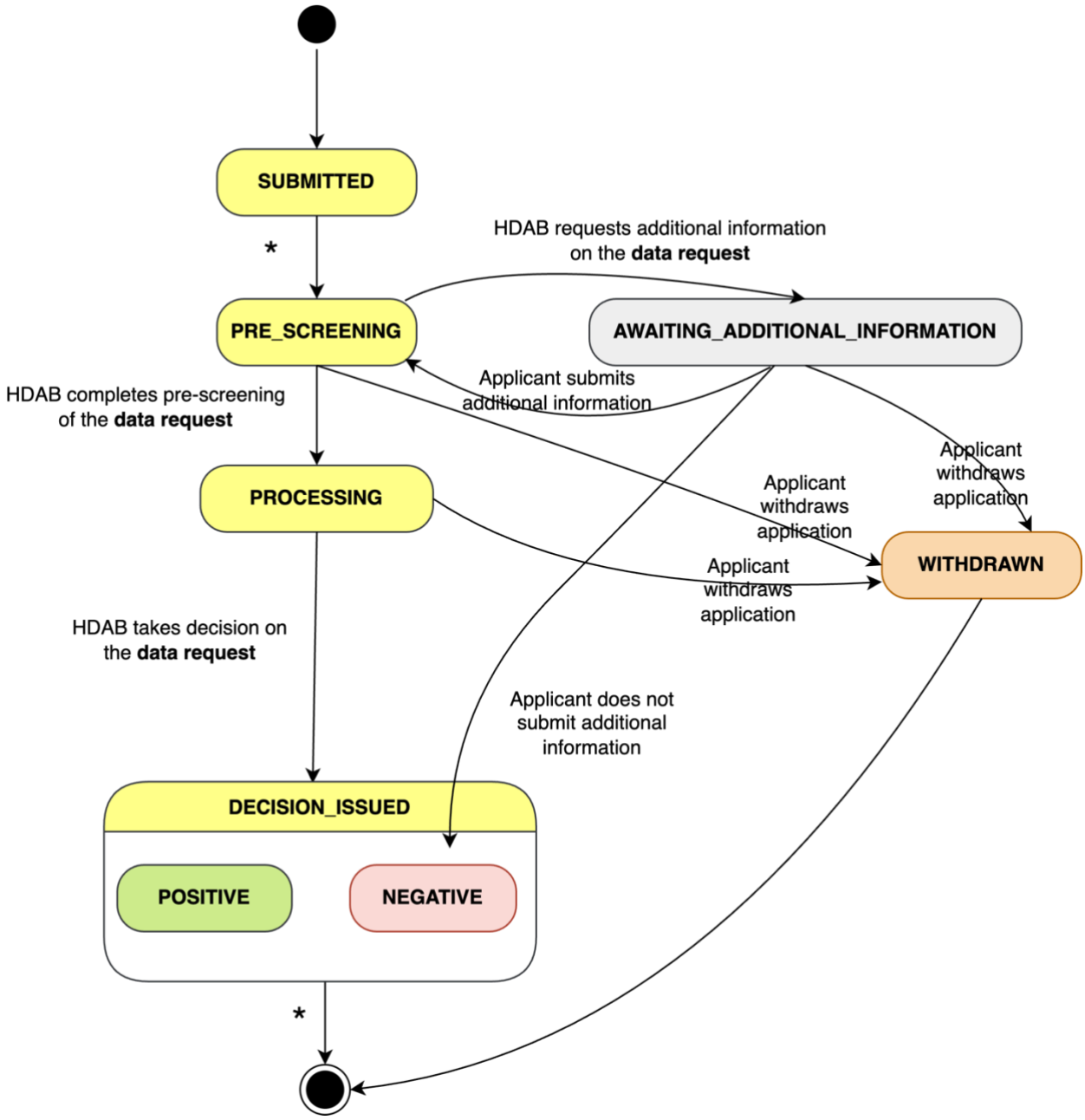
7.7 Updating the status of Data Request

DAAMS MUST allow authorized HDAB personnel to update the status of received data requests The statuses listed below are those that MUST be supported for data requests originating from the HealthData@EU Central Platform.

For Data Requests the following states are supported:

VALUE	Human readable	Description
SUBMITTED	Submitted	A application of type data request has been submitted and has been received by a DAAMS.
PRE_SCREENING	Pre screening	The application is undergoing a pre screening
PROCESSING	Processing	The application has been seen by an HDAB member and is being assessed.
AWAITING_ADDITIONAL_INFORMATION	Awaiting additional information requested by the HDAB	HDAB has marked the application as incomplete, and the health data applicant must provide necessary information
DECISION_ISSUED	Decision has been issued	A decision for the access application has been made.
WITHDRAWN	Withdrawn	An application has been withdrawn

Figure 2 Data Request State Machine Diagram



For data requests received from the HealthData@EU Central Platform DAAMS MUST send the following information to the NCP:

https://health-data-national-dispatcher.< *localhostname* >/#operation/<changeStatus>

Data Request Decision	
DAAMS → NCP → HealthDATA@EU CP	
Attributes	**Description**
Application ID	unique identifier of the data request
Status	Updated status of the data request

When the applicant has decided to withdraw their application, DAAMS will receive the following message:

Data Request Withdrawal	
HealthDATA@EU CP →NCP → DAAMS	
Attributes	**Description**
Application ID	unique identifier related to the acknowledged Application

8 Setting due dates

DAAMS MUST automatically identify and read the timestamps in the application

DAAMS MUST calculate all due dates for all steps of the process in accordance with the EHDS Regulation and starting from the timestamp of submission. Differences in the type of application workflow, e.g. accelerated procedure, normal procedure, Trusted Health Data Holder procedure, need to be considered.

DAAMS MUST support configurable internal timelines for handling applications, to allow Health Data Access Bodies to implement accelerated data access procedures as defined in Article 69 of the EHDS Regulation.

DAAMS MUST support the re-routing of applications that are not eligible for the accelerated procedure to the standard data access procedure.

DAAMS SHOULD enable notifications of upcoming due dates to be sent to the relevant assessment personnel to support timely processing and ensure compliance with the EHDS Regulation.

DAAMS MUST allow for due dates updates after following events: assessment extension, additional information requested, requested additional information received, decided, respond to a decision received.

For applications coming from the HealthData@EU Central Platform DAAMS MUST calculate due dates based on the timestamp received by the national DAAMS. For applications coming from the HealthData@EU Central Platform DAAMS MUST send the following information to the NCP in case the HDAB asks for an extension in the decision process as in the Art. 67,69:

https://health-data-national-dispatcher.<localhostname>/#operation/<setDueDates>

Extension request	
DAAMS → NCP → HealthDATA@EU CP	
Attributes	**Description**
Application ID	unique identifier of the data request

DAAMS MUST require documentation of the reasons for extensions of the due dates for the assessment of a Data Access Application and Data Request.

DAAMS MUST allow for the voiding of the due date when the status is set to AWAITING_ADDITIONAL_INFORMATION. Further, when the application status is changed from AWAITING_ADDITIONAL_INFORMATION to PROCESSING, the DAAMS MUST allow for the due date to be calculated based on the timestamp of when the application was updated with the additional information.

DAAMS SHOULD monitor all pending data access applications and data requests to detect cases where no decision has been made within a reasonable timeframe. For applications from the HealthData@EU Central Platform, reminders MAY be triggered by the Central Platform and relayed via the NCP._For national cases, DAAMS SHOULD implement an internal mechanism to generate such reminders and route them to the relevant HDAB personnel, in order to ensure timely processing and compliance with Article 40(5) of the EHDS Regulation.

9 Issuing a decision for Application

Once the HDAB has decided on an application or an application has been withdrawn by the applicant, DAAMS MUST allow authorized HDAB personnel to issue a formal decision.

https://health-data-national-dispatcher.<*localhostname*>/#operation/updateApplicationDecision

Decision	Description
Positive	Application is approved
Negative	Application has been rejected

DAAMS MUST support generating decisions in the templates developed by the Commission and referred to in Article 70 of EHDS regulation.

Decisions MUST be stored in the DAAMS. This decision MUST be saved as a signed, time-stamped document (e.g. PDF) and linked to the application record.

The decision MUST have an ID that is linked to a specific application ID.

For applications originating in the Central Platform, the DAAMS MUST send the decision and associated metadata to the Central Platform via NCP using the following message structure:
...

Decision Issued	
DAAMS → NCP → HealthData@EU CP	
Attribute	**Description**
Application ID	Unique identifier of the Application on the HD@EU Central Platform
Decision	Positive / Negative
Timestamp	DD:MM:YYYY
User	Firstname Lastname, Job title. HDAB personnel who signs the final decision.

Message structure for an acknowledgement sent by NCP to DAAMS after ingesting the previous message above:

Decision issued ACK	
HealthDATA@EU CP →NCP → DAAMS	
Attributes	**Description**
Application ID	unique identifier related to the acknowledged Application

9.1 Permit Pending Acceptance

In respect of positive decisions to data access applications, HDABs SHOULD provide the applicant with the final permit conditions and request confirmation before issuing the data permit. This enables the applicant to withdraw the application before activities such as data extraction and SPE creation begin; therefore reducing the admin burden and associated generation of costs.

In this case, DAAMS SHOULD be enabled to issue permit conditions pending acceptance by the applicant.

If the applicant declines, no permit is issued, and the application is considered withdrawn. DAAMS SHOULD support this optional confirmation step to avoid unnecessary data preparation and ensure clear communication.

In the event the applicant does not explicitly confirm acceptance or decline within a reasonable timeframe to be decided at MS level, the application MAY be considered to have been withdrawn.

If the applicant has accepted conditions, DAAMS MUST proceed to issue a data permit in accordance with EHDS Regulation.

9.2 Data permit status

The DAAMS MUST support following Data Permit statuses:

Status	Description
GRANTED	Data Permit has been issued and accepted
AMENDED	Amendments on a Data Permit have been made
RENEWED	Data Permit has been extended
REVOKED	Data Permit has been revoked
EXPIRED	Data Permit has expired

DAAMS MUST use the permit statuses to create a log of a permit through its lifecycle.

The DAAMS MUST support archiving and retrieval of all versions of a data permit. This must include automatically logging the dates each version of the permit was active.

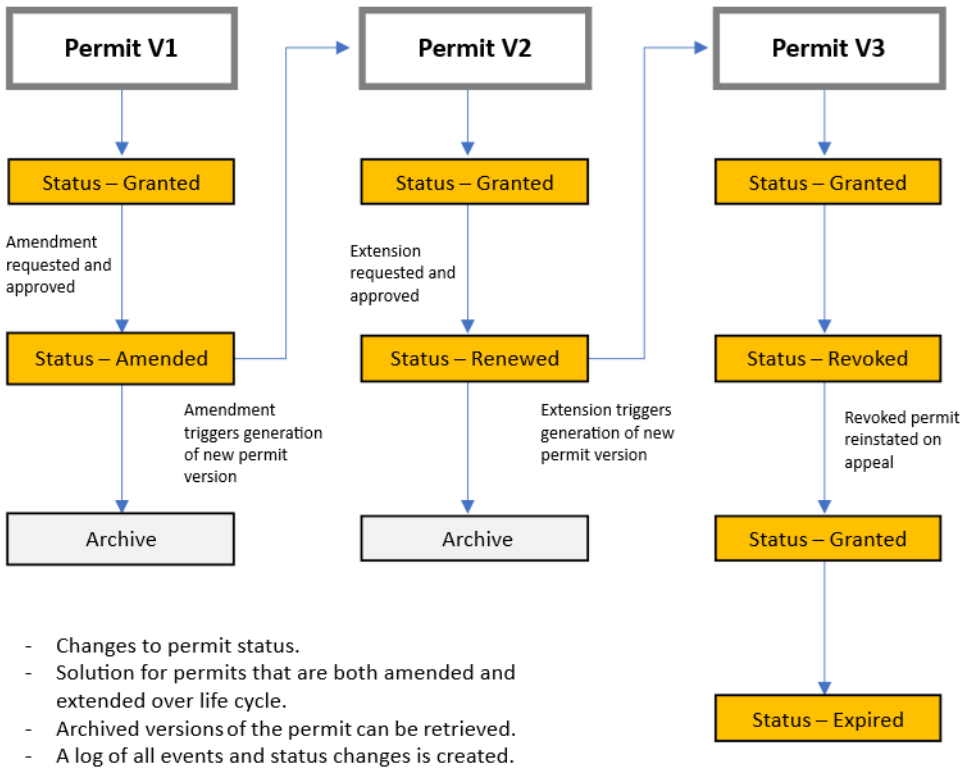
DAAMS MUST enable authorised HDAB personnel to change the status of a permit.

When the status of a data permit changes to AMENDED or RENEWED, the DAAMS must support the generation of a new unique permit ID for the AMENDED or RENEWED data permit.

When the status of a data permit is changed to AMENDED or RENEWED DAAMS MUST support generating the up-to-date permit for transmission to the data user, data holder and SPE provider.

The DAAMS MAY be configured to automatically issue alerts to HDAB personnel upon the expiry of a data permit.

Figure 3: Life cycle of permit that is amended, renewed and revoked over its life cycle.



After a decision

Permit amendments

DAAMS MUST enable the HDAB to document that a data user has applied for a permit amendment.

DAAMS MAY be configured to enable requests for amendment to be submitted directly to DAAMS. Otherwise, DAAMS must enable the justification provided by the data user to be stored and linked to the application record.

DAAMS MUST enable the HDAB to document its decision to a request for amendment and to associate this with the application record.

DAAMS MUST enable the HDAB to document and list the amendments approved.

Permit extension

DAAMS MUST enable the HDAB to document that a data user has applied for a permit extension.

DAAMS MAY be configured to enable requests for extension to be submitted directly to DAAMS. Otherwise, DAAMS must enable the justification provided by the data user to be stored and linked to the application record.

DAAMS MUST enable the HDAB to document its decision to a request for extension and to associate this with the application record.

DAAMS MUST NOT allow a permit that has been extended to be extended a second time.

Permit revocation

DAAMS MUST enable the HDAB to set a permit status to REVOKED.

DAAMS MUST enable the HDAB to document its justification for revocation and to link this to the application record.

In order to support timely cessation of processing, DAAMS MAY support generation of structured communications to the SPE operator and data user when a permit is revoked.

10 Processing decision appeals for Application

Member States MUST create national procedures enabling data applicants to appeal negative decisions.

The ability to appeal applies equally to data access applications and data requests.

It is not possible for data applicants to appeal a positive decision or to appeal the conditions applied to data access by the HDAB in accordance with Article 68(10). Neither is it possible to appeal in the case of an application that has been withdrawn by the applicant.

DAAMS MUST provide information on appeal mechanisms, either in the decision message or via the user interface or both.

The appeal mechanism MAY be integrated into DAAMS as a business flow or conducted through other channels such as email or in writing.

DAAMS MUST enable the formal, signed decision on the appeal (e.g. PDF) to be linked with the application record.

When an appeal is submitted for an application originating from the HealthData@EU Central Platform, DAAMS MUST be able to process the incoming message via the NCP. DAAMS MUST then send a confirmation of receipt to the HealthData@EU Central Platform.

Message structure for a notification of an appeal from the Central Platform to DAAMS :

Appeal to Issued Decision	
HealthData@EU CP → NCP → DAAMS	
Attributes	Description
Application ID	Unique identifier of the Application on the HD@EU Central Platform
User	name of the user who submitted the Application
Text	Text of the appeal
Date	Date DD:MM:YYYY of when the appeal was received by HDAB
Application Type	Data Access Application / Data Request

Message structure for an acknowledgement sent by DAAMS to the Central Platform after ingesting the previous message above:

Appeal to Decision Issued ACK	
DAAMS → NCP → HealthDATA@EU CP	
Attributes	**Description**
Application ID	unique identifier related to the acknowledged Application
Date acknowledged	Time DD:MM:YYYY of when the Data Access Application was acknowledged by DAAMS

11 Fetching related Data Permits for Mutual Recognition

DAAMS MAY fetch already issued Data Permits from the central registry and display them to the HDAB personnel as per Art 68.

12 Support for Trusted Data Holders

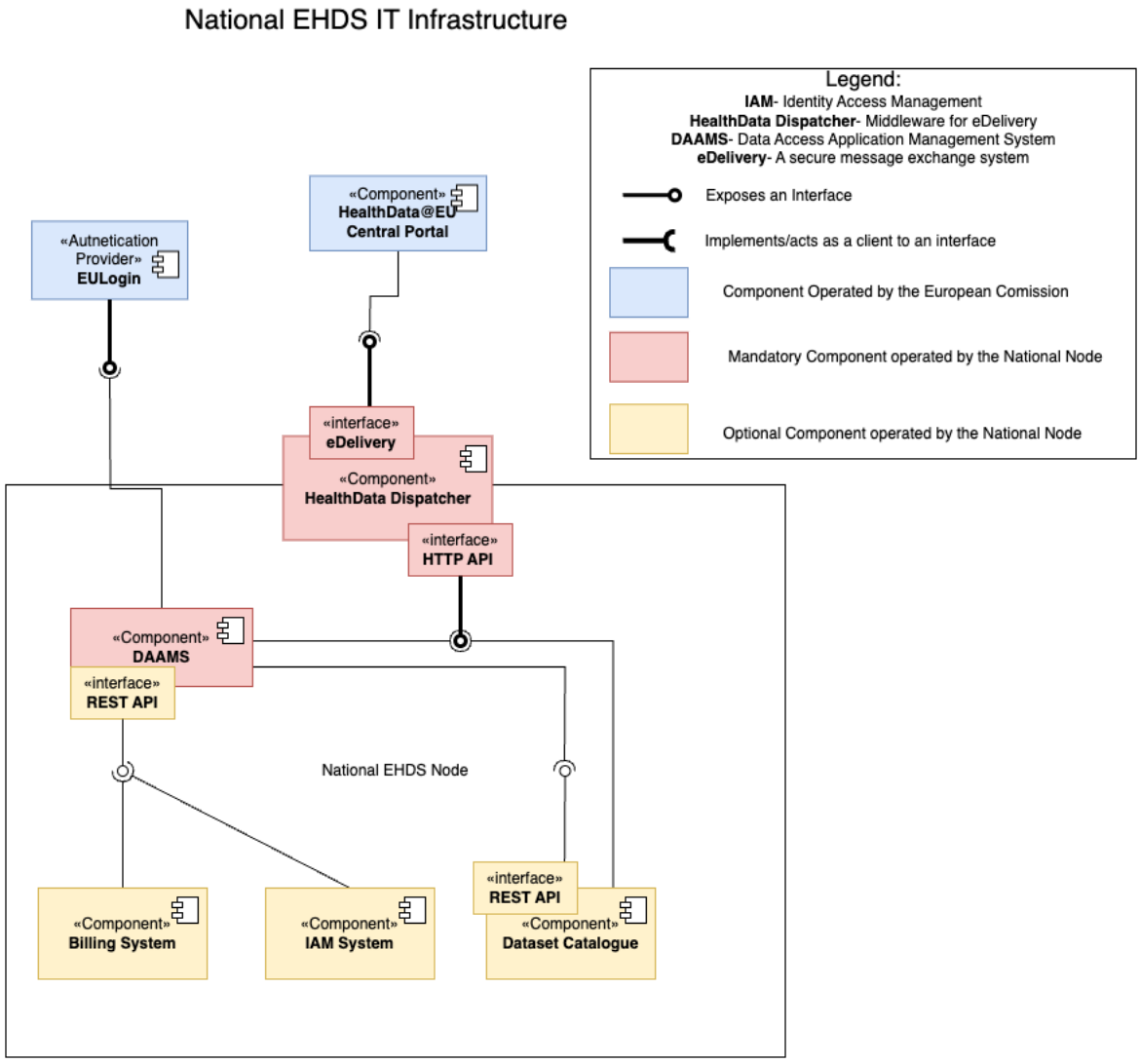
DAAMS MAY support involvement of Trusted Data Holders in the assessment phase. This MAY be done through a graphical user interface or by providing APIs that can be integrated into external systems.

Where DAAMS supports involvement of Trusted Data Holders, DAAMS MUST support transfer of applications or provide access to them to Trusted Health Data Holders for assessment.

If DAAMS supports involvement of Trusted Health Data Holders, DAAMS MUST also support receiving assessments and proposal for decision from the Trusted Health Data Holder.

13 DAAMs within National EHDS IT Infrastructure

Figure 4 Example National EHDS Infrastructure



The processing of data access applications and data requests incoming from the HealthData@EU Central Platform is illustrated in the message sequence diagram in Figure 2. The interaction involves three components: the HealthData@EU Central Platform, the HealthData Dispatcher (a communication gateway of the National Contact Point (NCP)), and the national DAAMS instance.

DAAMS MUST NOT communicate directly with the HealthData@EU Central Platform. All cross-border communication must flow through the National Contact Point which acts as the sole interface between national infrastructure and HealthData@EU Central Platform. This strict separation is essential to ensure consistent integration, regulatory compliance, and end-to-end traceability.

All messages exchanged between the NCP and the Central Platform, MUST follow the standard message formats defined under the HealthData@EU infrastructure. These include structured message types, which ensure semantic interoperability, consistency, and auditability across all national nodes.

The sequence can proceed as follows, but the communication is not limited to the sequence bellow:

1. Central Platform sends the application to the NCP

The HealthData@EU Central Platform validates and sends a standardised message containing a data access application or data request to the National Contact Point (NCP) of the destination Member State.

2. NCP forwards the application to DAAMS

The NCP receives the message, validates its structure and content, and sends it to the appropriate DAAMS instance. The message includes structured data and supporting documentation such as applicant identity, legal basis, purpose of use, dataset references, and annexes.

3. HDAB processes the application in the DAAMS

The HDAB processes the application in the DAAMs in accordance with applicable national procedures and legal requirements, in line with Articles 51 and 53 of the EHDS Regulation.

4. DAAMS sends status updates to the NCP

Throughout the application lifecycle, the DAAMS sends status updates (e.g. Submitted, Pre screening, Processing, Awaiting Additional Information, Decision issued, Withdrawn) to the NCP.

The NCP then sends these updates to the HealthData@EU Central Platform using standardised HealthData@EU messages to keep the applicant informed.

5. DAAMS sends the decision to the NCP

Once the HDAB has made a decision (approval or rejection), the DAAMS sends a structured decision message to the NCP, including any justification, conditions, or applicable time limits.

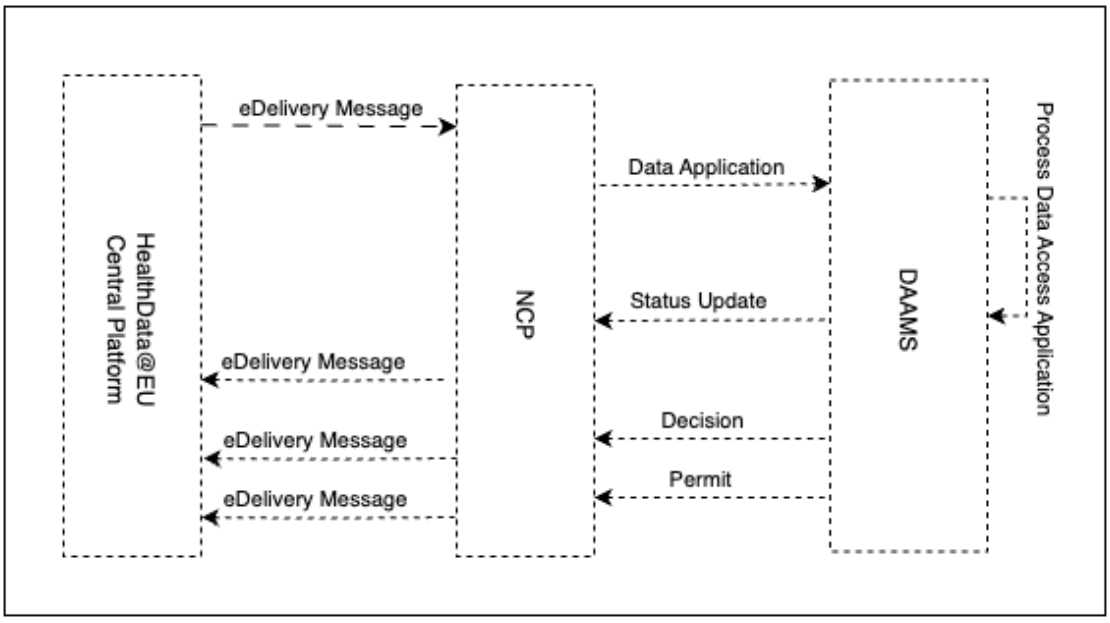
NCP then forwards this decision to the HealthData@EU Central Platform

6. DAAMS issues the permit and sends it to the NCP

If access is granted, the HDAB issues a data permit in the standard EU format. The permit is transmitted from the DAAMS to the NCP, which then sends it to the HealthData@EU Central Platform for delivery to the applicant.

This communication model ensures that all message exchanges remain traceable, secure, and fully aligned with the interoperability requirements defined in the EHDS Regulation.

Figure 5 Message Sequence Diagram depicting the communication between DAAMS, NCP and HealthData@EU Central Platform. Note that not all messages are illustrated.



14 Non-functional Requirements

This section lists all non-functional requirements that a DAAMS MUST or SHOULD fulfil.

14.1 Time zone/Timestamps

All system-generated timestamps SHOULD be recorded in Coordinated Universal Time (UTC) and expressed using the ISO 8601 extended format (e.g. 2025-05-19T14:23:00Z).

Timestamps MUST include date, time, and time zone offset or the Z (Zulu) suffix for UTC.

The system MAY display local time to users for convenience but MUST store and exchange all timestamps in UTC.

All logs, application lifecycle events, permit records, and status updates exchanged via APIs MUST use UTC timestamps to ensure consistency across Member States.

Where applicable, the system SHOULD synchronise its internal clock using NTP (Network Time Protocol) with a reliable time source.

14.2 Graphical User Interface

The system MUST provide a Graphical User Interface (GUI) that is accessible to authorised users, including HDAB personnel and other relevant roles involved in the data access workflow. The GUI MUST support role-based access control, presenting functionality and information appropriate to each user's permissions and responsibilities.

14.3 System load

DAAMS MUST be capable of handling expected volumes of concurrent access requests and data processing operations without unacceptable performance degradation. It SHOULD support load balancing and dynamic resource scaling to ensure consistent responsiveness, availability, and reliability under varying and peak load conditions. DAAMS MUST be able to maintain acceptable response times under normal and peak load conditions.

14.4 Auditing

Auditing in DAAMS MUST ensure transparency, accountability, and compliance in processing health data access applications and data requests. DAAMS MUST log key events—such as user access, application submissions, decision-making steps, data permit issuance, and changes to access permissions. These logs MUST be immutable and accessible only to authorized personnel, providing a secure, verifiable trail which allows alignment with legal requirements and corresponding business rules.

The auditing SHOULD cover events listed, but not limited to, the following:

- Application submission and modifications
- Evaluation steps and reviewer actions
- Access decisions (approval/rejection)
- Permit generation and delivery
- Any user or system interaction that affects the decision issuing process

14.5 Authentication and Authorization Management

DAAMS MUST be protected against unauthorized access; therefore, it MUST implement authentication and authorization mechanisms appropriate for the submission and processing of data access applications and data requests for secondary use.

DAAMS SHOULD use an eIDAS-compliant electronic identification and authentication provider to authenticate natural persons and legal entities submitting data access applications or data requests.

The chosen authentication mechanism MUST enable authorization management of HDAB personnel. Thus, ensuring only authorized people can process data access applications and data requests in line with national processes and legislation.

14.6 API

The system SHOULD expose an API that can be used by authorized users to interact with DAAMS. The API implementation is entirely under the control of the Member State. It is recommended to use widely adopted web standards such as REST over HTTPS with JSON payloads, ensuring maintainability, security, and ease of integration. Member States may choose any architecture or framework that suits their national requirements, provided the interoperability with the Central Platform—via the NCP—is preserved using the standardised interfaces defined at EU level.

15 Security Considerations

DAAMS MUST support audit logging of security-relevant events.

DAAMs MUST implement mitigations for common OWASP Top 10 threats. Implementers MUST read these references regularly in detail and apply the countermeasures described therein.

16 Open questions and unresolved issues

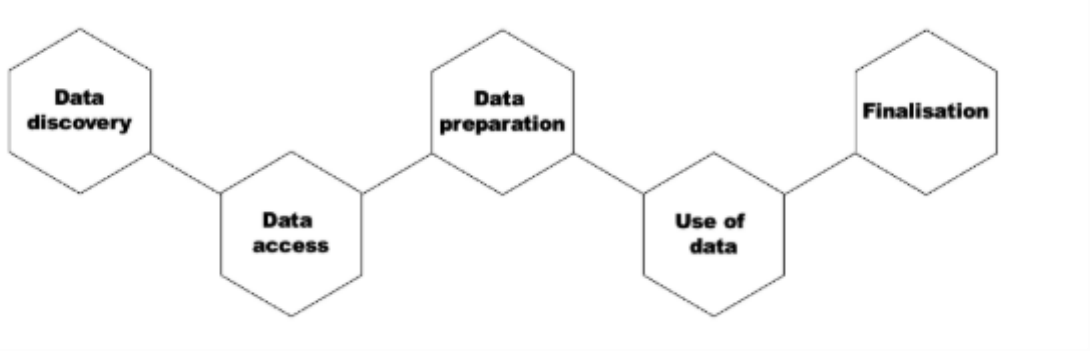
- Digital Representation of a data permit
    - There is currently no legal obligation for the data permit to be represented in a structured digital format such as JSON or XML.
    - Article 70 of the EHDS Regulation foresees an implementing act that will define the content and template of the permit, but it does not prescribe a specific technical format like a machine-readable schema.
    - The permit must be issued in an electronically readable format (e.g. digitally signed PDF), and Member States may also choose to implement a structured version (e.g. XML/JSON) to facilitate processing or reporting — but this remains optional.
- How does appeal work and how does it translate to DAAMS? Specifically if the applicant withdraws from the application, is it a negative decision? They can withdraw because they did not agree to HDAB conditions.

17 Annexes

17.1 Annex 1 - 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
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.

17.2 Annex 2 - 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**.

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))
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.
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, 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))
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)
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.
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 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 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-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.
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 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 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)
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)
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 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 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**.