D6.4 Data Access Application Management System (DAAMS) – Technical specification for health data access bodies

TEHDAS2 – Second Joint Action Towards the European Health Data Space

24 March 2026

Co-funded by the European Union

0 Document info

0.1 Authors

Author(s)	organisation
Radovan Tomášik (Lead author)	Ministry of Health of the Czech Republic, Czech Republic (Lead organisation)
Zdenek Gütter	Ministry of Health of the Czech Republic, Czech Republic (Lead organisation)
Pinar Alper	Luxembourg National Data Service, Luxemburg
Azul O'Flaherty	Department of Health, Ireland
Sam Santosh	Maynooth University, Ireland
Richard Hrabčák	National Health Information Centre (NCZI), Slovakia
Ana Martin-Moreno	Ministry Of Health of Spain, Spain
Normunds Kante	Latvian Biomedical Research and Study Centre, Latvia
Ana Muzinic	Federal Institute for Drugs and Medical Devices, Germany
Karel Winderickx	Belgian Health Data Agency, Belgium
Maria Athanasaki	GRNET, Greece
Dimitris Kalogeras	GRNET, Greece
Yannis Skopoulis	GRNET, Greece
Nicoletta Prentzas	CYENS, Cyprus
Tomasz Stachurski	e-Health Centre, Poland

0.2 Keywords

Keywords	TEHDAS2, Joint Action, Health Data, Health Data Space, HDAB, DAAMS, Application Management

0.3 Document history

Date	Version	Editor	Change	Status
27.02.2026	0.5	Radovan Tomasik	Feedback from the public consultation	DRAFT
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

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

The text is based on the Official Published Version of the Regulation.

The document also follows the recommended structure of TEHDAS2 Handbook for Deliverables.

Copyright Notice

Contents

1 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 (EU), 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 a national level. It manages the full application and decision 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 HDABs in the EU 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.

2 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 Data Protection Board	EDPB
European Health Data Space	EHDS
European Union	EU
European Union Agency for Cybersecurity	ENISA
General Data Protection Regulation	GDPR
Geospatial Data Catalogue Application Profile	GeoDCAT-AP
Graphical User Interface	GUI
Health Data Access Body	HDAB
Data Access Application Management System	DAAMS
Secure Processing Environment	SPE
European Interoperability Framework	EIF
Health Data Catalogue Vocabulary Application Profile	HealthDCAT-AP
Joint Action	JA
Minimum Viable Product	MVP
National Contact Point for Secondary Use	NCP
Portable Document Format	PDF
Statistical Data Catalogue Vocabulary Application Profile	StatDCAT-AP
The Finnish Innovation Fund	Sitra

Trusted Data Holder	TDH
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

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 behavior 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 personalised notifications on data access events."

4 Terminology definition

IMPORTANT NOTE TO READERS: The terminology definitions are listed in Annex 4 (Glossary) and constitute a normative portion of this specification, imposing requirements upon implementations. All capitalised words in the text of this specification – such as “Data Permit” – refer to the terms defined in Annex 4. Whenever the reader encounters such capitalised words, the definitions provided in Annex 4 MUST be followed. For more context on 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 EHDS Regulation. User journey depicting intended use of EHDS is detailed in Annex 3.

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.

This document that was created according to the methodology outlined in Annex 1, should be understood as an expert opinion and guidance document developed within the TEHDAS2 framework, reflecting technical and expert input from the project partners, as well as results of the public consultation listed in Annex 2. It is not legally binding and does not constitute a formal guideline or technical specification under the EHDS.

This document does not represent the position of the European Commission.

Legally binding and enforceable requirements under the EHDS are laid down in Regulation (EU) 2025/327 and, where applicable, in implementing acts adopted by the European Commission, within the limits of the empowerments provided by the Regulation.

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 DAAMS in accordance with the EHDS Regulation.

DAAMS serves as a national platform managed by 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 EU 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 application programming interfaces (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 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 HDAB, this specification focuses on the DAAMS component responsible for the submission and processing of Health Data Access Applications and Health Data Requests.

Specifically, DAAMS is software used by the HDAB to support two main functions:

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

This specification does not require that all functions relevant to the work of an HDAB be implemented within DAAMS itself. Member States may fulfil certain HDAB obligations through separate but interoperable systems, provided that compliance with the EHDS Regulation remains demonstrable and that legal traceability, auditability and accountability are preserved across system boundaries.

Accordingly, the following may be implemented outside DAAMS where appropriate under national level architecture:

- National electronic health data catalogues and dataset discovery tools.
- Secure processing environments (SPEs) and other secure data processing infrastructures.
- National public information or transparency portals.
- National complaint handling systems or other administrative redress tools.
- National Dispatcher services and related HealthData@EU interoperability components.
- National authentication, authorisation and identity management provider.

Where such functions are implemented outside DAAMS, DAAMS MUST, as relevant to its role in application and permit management, support the recording, exchange or linkage of the information necessary to maintain an auditable end-to-end case record.

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 IT Infrastructure for processing of Health Data Access Applications.

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 standardised DAAMS 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 health data access application, health data request and decision related information across Member States and the entire federated EHDS IT infrastructure. The DAAMS is designed to technically facilitate the procedural workflows detailed in the TEHDAS D6.3 guideline.

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 standardisation 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, as required by the regulation.
- **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.This document, where relevant, refers to the HealthData@EU National Dispatcher OpenAPI specification to identify the details of information exchanges.

Out of scope are national-level implementation details, internal decision-making processes of HDABs , and the operation of secure processing environments (SPEs). 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. Interoperability requirements are defined in this document at the functional and process level; however, the detailed API definitions, including versioning and change management, are specified separately. Implementers SHALL refer to the HealthData@EU National Dispatcher OpenAPI specification [1]as the normative source for these interface details.

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 health 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

6.1 Applicant user space

R6.1.1 DAAMS MUST provide a unified graphical user interface (GUI) web interface among components through which applicants can place national health data access applications or health data requests.

R6.1.2 DAAMS GUI web interface MUST support at least one official language of the EU , and, in addition, it SHOULD also support the English language.

R6.1.3 DAAMS GUI web interface SHOULD allow the applicant to configure the language settings.

R6.1.4 DAAMS MUST provide a user space for applicants to create draft application forms, submit applications, track application status, and complete applications by providing additional information.

R6.1.5 DAAMS MUST provide applicants with an overview of all their applications, including application status and key milestones or deadlines. DAAMS MAY provide this overview through an application dashboard with visual indicators of status, progress, timelines, and expected next actions.

[1] https://health-data-national-dispatcher.acceptance.data.health.europa.eu/

R6.1.6 DAAMS MUST allow the applicants to download documents attached to their applications by the HDAB. e.g. decision documents in the case of rejection of applications or e.g. permit documents in case of approved data access applications.

R6.1.7 DAAMS user space SHOULD provide a messaging interface facilitating exchanges between the applicant and the HDAB assessor, while ensuring auditability and data protection.

R6.1.8 DAAMS web interface SHOULD 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.

R6.1.9 DAAMS MUST support push notifications on every change of application status with clear explanation of what the change means and the required actions.

R6.1.10 DAAMS MUST, at a minimum, offer push notifications in Email and in In-app format.

R6.1.11 DAAMS MUST allow the applicant to view all In-app notifications ordered by their timestamps.

R6.1.12 DAAMS MAY allow the applicant to search by free text over applications and notifications in their user space.

6.2 Creating applications

R6.2.1 DAAMS MUST provide respective templates/forms to allow applicants to create health data access applications or health data requests.

R6.2.2 DAAMS MUST allow users to create a health data access application or a health data request for one or more datasets described in the National Health Dataset Catalogue.

R6.2.3 DAAMS MAY adopt the commonplace “shopping cart” metaphor to allow users to select multiple datasets prior to creating a health data access application (or health data request).

R6.2.4 For each dataset included in a health data access application (or health 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.

R6.2.5 The health data access application form provided by the DAAMS MUST match the information requirements of the EU Common Health Data Access Application form. These forms will be further specified by implementing acts adopted under Article 70 of the EHDS Regulation.

R6.2.6 The health data 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.

R6.2.7 The health data request form provided by the DAAMS MUST match the information requirements of the EU Common Health Data Request form. These forms will be further specified by implementing acts adopted under Article 70 of the EHDS Regulation.

R6.2.8 The health 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.

R6.2.9 DAAMS SHOULD guide the applicant in filling out the form by ordering the presentation of form fields in sections.

R6.2.10 DAAMs MUST guide the applicants by providing section-by-section tracking of form completeness.

R6.2.11 DAAMs MUST provide help feature with inline guidance on form sections and fields.

R6.2.13 DAAMS MAY automatically populate fields concerning applicant information using applicant's login profile.

R6.2.14 DAAMS MUST highlight mandatory form fields and display field guidance text to assist the applicants when filling in forms.

R6.2.15 DAAMS MUST provide appropriate field validations functions and display validation errors to the applicant as messages.

R6.2.16 DAAMS MUST allow applicants to save forms as draft (without submitting them) so that they can continue filling the form later.

R6.2.17 DAAMS MUST allow applicants to modify a previously saved draft form.

R6.2.18 DAAMS MUST allow applicant to view all draft forms in their user space.

R6.2.19 DAAMS MUST allow applicants to cancel (or delete) a draft application form.

R6.2.20 DAAMS MUST support HDAB-defined business rules regarding expiry of draft forms, e.g., a draft form not submitted within 6 months shall expire.

R6.2.21 DAAMS MUST notify applicants when their draft forms will expire due to extended period of inactivity.

R6.2.22 DAAMS MUST allow applicant to print draft and submitted forms.

R6.2.23 DAAMS SHOULD allow the applicant to create a draft copy (or clone) from another draft form.

R6.2.24 DAAMS MAY allow populating draft forms by importing from form exports that are in a machine-actionable format.

R6.2.25 DAAMS SHOULD allow applicants to add additional datasets to a draft health data access application (or health data request) form.

R6.2.26 DAAMS MUST NOT allow the submission of a form that is missing required fields or has field validation errors.

R6.2.27 DAAMS SHOULD highlight to the applicant when all required fields (in all sections) of the form are complete, and all field validations are successful.

6.3 Submitting applications and providing additional information

R6.3.1 DAAMS MUST allow the applicant to submit an application.

R6.3.2 DAAMS MUST allow the applicant to track status of their application(s), including at a minimum, the states identified in Section 7.6 of this specification.

R6.3.3 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 4 weeks to provide additional information on an application that has been sent back to them for completion by the HDAB.

R6.3.4 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).

R6.3.5 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.

R6.3.6 Per form field flagged by the HDAB, the DAAMS MUST allow the applicant to enter the required further information and save the form.

R6.3.7 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").

R6.3.8 DAAMS MUST allow the applicant to withdraw a submitted application.

R6.3.9 DAAMS MUST allow export of submitted forms in a machine-actionable format.

R6.3.10 DAAMS MUST notify or show the applicant about fees estimates plus the option to withdraw, with only already-incurred costs chargeable.

7 Processing applications – DAAMS back office

7.1 Handling of applications from HealthData@EU Central Platform via national contact points

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 national contact point (NCP) when a user submits them. DAAMS MUST NOT communicate directly with the HealthData@EU Central Platform.

For applications submitted through the HealthData@EU Central Platform and subsequently received and processed by national DAAMs, the message structures enabling communication between Member States' NCPs and the HealthData@EU Central Platform are defined in the National Dispatcher OpenAPI specification.

HealthData@EU National Dispatcher OpenAPI specification[2]: member states can find and interact with this API, which 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.

[2] https://health-data-national-dispatcher.acceptance.data.health.europa.eu

R7.1.1 DAAMS MUST allow access to the received applications only for authorised personnel.

R7.1.2 For applications submitted via the HealthData@EU Central Platform, the national DAAMS MUST be able to ingest applications in the languages submitted via the central platform. Each application message MUST specify the application language

R7.1.3 For applications placed via the national DAAMS;

- the DAAMS MUST accept applications in the national language(s) of the HDAB,
- the DAAMS SHOULD accept applications in English.

7.2 Pre-screening by HDAB

R7.2.1 DAAMS MUST enable HDAB personnel to conduct a pre-screening of applications, including both health data access applications and health data requests. TEHDAS guideline 6.3 outlines the steps that should be taken to conduct pre-screening of applications.

R7.2.2 DAAMS MUST enable the HDAB personnel to document the outcome of the completeness check.

R7.2.3 DAAMS MUST enable applications deemed complete to proceed to assessment.

R7.2.4 DAAMS MUST enable the completeness check result to be stored as a structured entry in the application record and made available for audit.

R7.2.5 DAAMS MUST enable applications deemed incomplete by the HDAB to be returned to the applicant for completion; or to be rejected.

R7.2.6 DAAMS MUST enable HDAB personnel to document a structured justification for rejection as incomplete.

R7.2.7 DAAMS MUST enable complete applications to proceed to assessment.

R7.2.8 DAAMS SHOULD allow HDAB personnel to flag applications, wherein the nature of datasets included in the application may result in sensitive information within the application or within the communications that occur during application assessment phase e.g. data protected by intellectual property rights, trade secrets or covered by the regulatory data as per Article 52.

R7.2.9 DAAMS SHOULD offer the possibility to run in a Restricted Mode for flagged applications. For applications under Restricted Mode, the DAAMS SHOULD prevent download, print, copy, or export of the application.

R7.2.10 In cases where the HDAB use the DAAMS as a communications platform among stakeholders related to the application, the DAAMS SHOULD allow;

- health data holder to record their communications with regards to applications concerning the data they hold,
- applicant to record communications with regard to the application they have submitted,
- HDAB to record their communications with regard to the applications they receive.

7.3 Application assessment by HDAB – health data access applications

R7.3.1 DAAMS SHOULD allow HDAB personnel to document the outcomes of HDAB assessments of health data access applications against the requirements in Article 68(1)(a)–(h), including providing justifications where needed. The data permit template in D6.3 already covers all points of Article 68(1), and completing the template should be sufficient for formal decisions.

R7.3.2 In addition to the overall decision document, DAAMS MAY 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.

R7.3.3 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.

R7.3.4 DAAMS MUST record the individual HDAB personnel member who conducted these assessments in part or in full.

R7.3.5 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.

R7.3.6 For multi-country applications submitted through the HealthData@EU Central Platform, the (national) DAAMs MUST allow the storage of information shared by other HDABs or authorised participants as document attachments.

R7.3.7 DAAMS MUST enable the HDAB to record its overall assessment of the application including justifications.

R7.3.8 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.

7.4 Application assessment by HDAB – health data requests

R7.4.1 DAAMS SHOULD allow HDAB personnel to document the outcomes of HDAB assessments of health data requests, including providing justifications where needed.

Completing the data request approval template in D6.3 guideline should be sufficient for formal decisions.

R7.4.2 In addition to the overall decision document, DAAMS MAY enable structured storage of the delivery conditions associated with the health 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. Further guidance on the HDABs public information duties will be provided in the TEHDAS2 document “M8.3 Guideline for Health Data Access Bodies on informing natural persons about the use of health data – Citizen Information Point”

R7.4.2 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.

R7.4.3 DAAMS MUST enable the HDAB to record and store its formal decision on the health data request. This decision MUST be saved as a signed, time-stamped document (e.g. PDF) and linked to the application record.

7.5 Requesting and receiving additional information for an application

R7.5.1 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.

R7.5.2 Upon receipt of the additional information, DAAMS MUST:

Update the status of the application to PRE_SCREENING or PROCESSING, based on the phase during which the request for additional information occurred (see Figure 1(b)).

Notify relevant HDAB personnel

Acknowledge receipt via a message to the Central Platform

R7.5.3 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.

7.6 Updating the status of applications

For applications submitted through the HealthData@EU Central Platform and subsequently received and processed by national DAAMs, the statuses and the operations enabling communication statuses between Member States' NCPs and the HealthData@EU Central Platform are defined in the National Dispatcher OpenAPI specification. D6.4 DAAMs specification provides context into statuses listed in the National Dispatcher OpenAPI specification and illustrates status transitions.

The status values for HealthData Access Applications and Health Data Requests are the same and are listed in Table 1(a). The corresponding state transitions are illustrated in Figure 1(a).

Table 1(a): List of statuses that MUST be supported for applications (both health data access applications and health data requests)

APPLICATION STATUS VALUE	Human readable label	Description
SUBMITTED	Submitted	The application has been submitted and has been received by the DAAMS.
PRE_SCREENING	Pre-screening	The application is undergoing a pre-screening where the HDAB is checking the application for completeness.
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 complete the application by providing the necessary information.
DECISION_ISSUED	Decision has been issued	A decision for the access application has been made.

WITHDRAWN	Withdrawn	The application has been withdrawn.

The status values concerning the decision lifecycle of for Health Data Access Applications and Health Data Requests are the same and are listed in Table 1(b). The corresponding state transitions are illustrated in Figure 1(a).

Table 1(b): List of statuses that MUST be supported for health data access applications during the decision phase (both health data access application and health data request)

STATUS VALUE	**Human readable label**	**Description**
POSITIVE_DECISION_ISSUED	Positive Decision Issued	The HDAB has issued a positive decision.
NEGATIVE_DECISION_ISSUED	Negative Decision Issued	The HDAB has issued a negative decision.
POSITIVE_DECISION_ACCEPTED	Positive Decision Accepted	The applicant has accepted the positive decision issued by the HDAB
NEGATIVE_DECISION_ACCEPTED	Negative Decision Accepted	The applicant has accepted the negative decision issued by the HDAB.
POSITIVE_DECISION_REJECTED	Positive Decision Rejected	The applicant has rejected the positive decision issued by the HDAB
NEGATIVE_DECISION_APPEALED	Negative Decision Appealed	The applicant has appealed the negative decision issued by the HDAB.
APPEAL_APPROVED	Appeal Approved	Applicant's appeal has been approved.
APPEAL_REJECTED	Appeal Rejected	Applicant's appeal has been rejected.

Figure 1(a): State machine diagram showing the transitions between the states (listed earlier in **Table 1(a))** an application can be in.

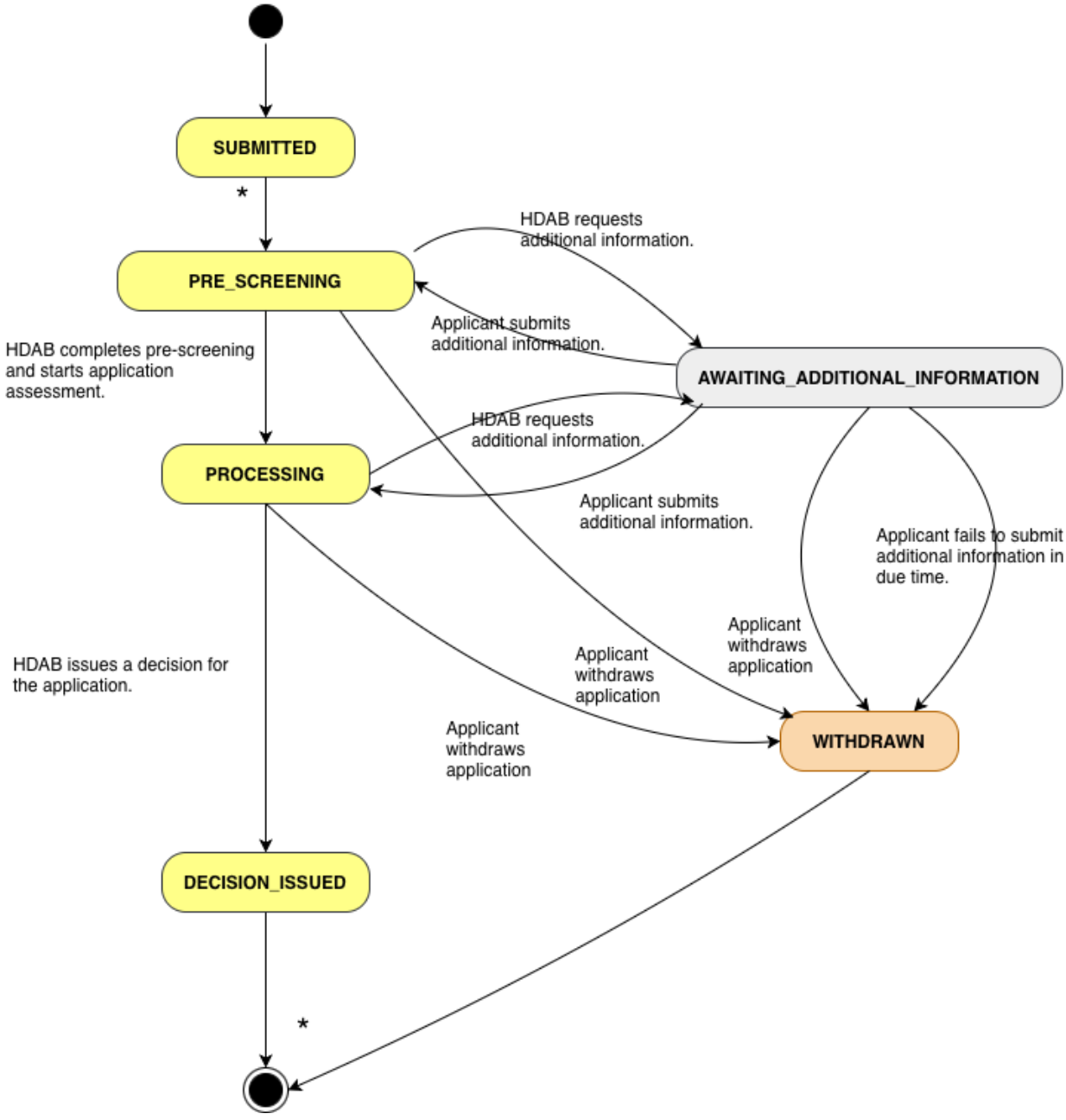


Figure 1(b): State machine diagram showing the possible states of an application decision and the transitions between the states (listed earlier in **Table 1(b)**).

R7.6.1 DAAMS MUST allow authorised HDAB personnel to update the status of received applications (both health data access applications and health data requests).

R7.6.2 As a minimum, the DAAMs MUST support the statuses listed in **Tables 1(a)** and **1(b)** for applications (both health data access applications and health data requests) originating from the HealthData@EU Central Platform.

R7.6.3 For applications (both health data access applications and health data requests) received from the HealthData@EU Central Platform DAAMS MUST communicate all application status transitions (in **Figures 1(a)** and **1(b)**) as status updates to the NCP.

8 Setting due dates

R8.0.1 DAAMS MUST automatically identify and read the timestamps in the application

R8.0.2 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.

R8.0.3 DAAMS MUST support configurable internal timelines for handling health data access applications, to allow HDABs to implement accelerated data access procedures as defined in Article 68(6) of the EHDS Regulation.

R8.0.4 DAAMS MUST enable authorised HDAB personnel to route eligible health data applications for an accelerated procedure instead of the standard procedure.

R8.0.5 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.

R8.0.6 DAAMS MUST allow for due date updates after following events: assessment extension, additional information requested and requested additional information received.

R8.0.7 For applications coming from the HealthData@EU Central Platform DAAMS MUST calculate due dates based on the timestamp received by the national DAAMS.

R8.0.8 DAAMS MUST require recording a written justification when the HDAB has extended the due date for assessment of a health data access application in accordance with article 68(4).

R8.0.9 DAAMS MUST enable transmission of the justification for extension of the application processing time to the applicant.

R8.0.10 DAAMS SHOULD monitor all pending health data access applications and health 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.

9 Issuing a decision for application

9.1 Generating and storing decisions

R9.1.1 Once the HDAB has decided on an application, DAAMS MUST allow the HDAB to issue a formal decision.

The statuses and the operations enabling communication statuses issued by the HealthData@EU Central Platform are defined in the National Dispatcher OpenAPI specification.

Table 2: Decision types that MUST be supported

Decision	Description
Positive	Application is approved
Negative	Application has been rejected

R9.1.2 DAAMS MUST support generating decisions in the templates developed by the Commission and referred to in Article 70 of EHDS Regulation.

R9.1.3 Decisions MUST be stored in the DAAMS. A decision MUST be saved as a signed, time-stamped document (e.g. PDF) and linked to the application record.

R9.1.4 DAAMS MUST assign an ID to each decision that is linked to a specific application ID.

9.2 Decision cards / Decisions pending acceptance

The term decision card refers to the structured format in which decision information is communicated to applicants via the HealthData@EU Central Platform.

Applications originating from the HealthData@EU Central Platform

R9.2.1 DAAMS MUST allow the HDAB to issue decision information to the HealthData@EU Central Platform in the structured format required for implementation of the decision card model.

R9.2.2 DAAMS MUST issue positive decisions to the HealthData@EU Central Platform as a pre-permit document enabling the applicant to review permit conditions in the form of a PDF of the unsigned data permit.

R9.2.3 DAAMS MUST issue negative decisions to HealthData@EU Central Platform as a PDF of the final decision, signed by authorised HDAB personnel.

R9.2.4 DAAMS MUST be enabled to receive messages from the HealthData@EU Central Platform via the NCP on whether the applicant has chosen to Accept, Reject, Appeal or failed to respond to the decision card.

National Applications

R9.2.5 DAAMS SHOULD enable the HDAB to issue decision information in the decision card format for national applications as well as for those originating in the HealthData@EU Central Platform. Providing notice of permit conditions enables the applicant to withdraw the application before activities such as data extraction and SPE creation begin; therefore, reducing the administrative burden and associated generation of costs.

R9.2.6 DAAMS SHOULD apply the same 28-day deadline as the HealthData@EU Central Platform for applicants to respond to a decision card.

R9.2.7 DAAMS MAY be configured to send reminders to the applicant during the response deadline.

R9.2.8 DAAMS SHOULD automatically withdraw applications where the applicant has not responded to a national decision card within 28 days. In the event an application is automatically withdrawn, DAAMS MUST update the application status to WITHDRAWN.

R9.2.9 DAAMS MAY be configured to issue a communication to the applicant confirming the application is withdrawn.

9.3 Data permit lifecycle

The statuses and the operations enabling communication statuses issued by the HealthData@EU Central Platform are defined in the National Dispatcher OpenAPI specification.

R9.3.1 The DAAMS MUST support data permit statuses as defined in the open API specification (table 3 below).

Table 3: Data permit statuses

Permit Status Value	Description
GRANTED	Permit has been granted
RENEWAL_REQUESTED	Renewal of permit has been requested
RENEWED	Permit has been renewed
RENEWAL_REJECTED	Renewal request was rejected
EXPIRED	Permit has expired
AMENDMENT_REQUESTED	Amendment to permit has been requested
AMENDED	Permit has been amended

AMENDMENT_REJECTED	Amendment request was rejected
REVOKED	Permit has been revoked
REVOKE_APPEALED	Revocation has been appealed
APPEAL_APPROVED	Appeal was approved
APPEAL_REJECTED	Appeal was rejected

R9.3.2 DAAMS MUST use the permit statuses to create a log of a permit through its lifecycle.

R9.3.3 DAAMS MUST automatically log the dates each version of the permit was active.

R9.3.4 The DAAMS MUST support archiving and retrieval of all versions of a data permit.

R9.3.5 DAAMS MUST enable authorised HDAB personnel to change the status of a permit.

R9.3.6 When an amendment request, renewal request or a permit revocation appeal are approved, DAAMS MUST support generating the up-to-date permit version for signature by the authorised HDAB personnel and transmission to the data user, data holder and SPE provider.

R9.3.7 DAAMS MUST support the generation of a unique permit ID for each new version of a data permit

R9.3.8 The DAAMS MUST generate unique permit IDs in a structured format that:

- Identifies the issuing HDAB
- Maintains a persistent base identifier
- Identifies amended or renewed permits as versions of the same base permit
- Reflects the chronological order of versions

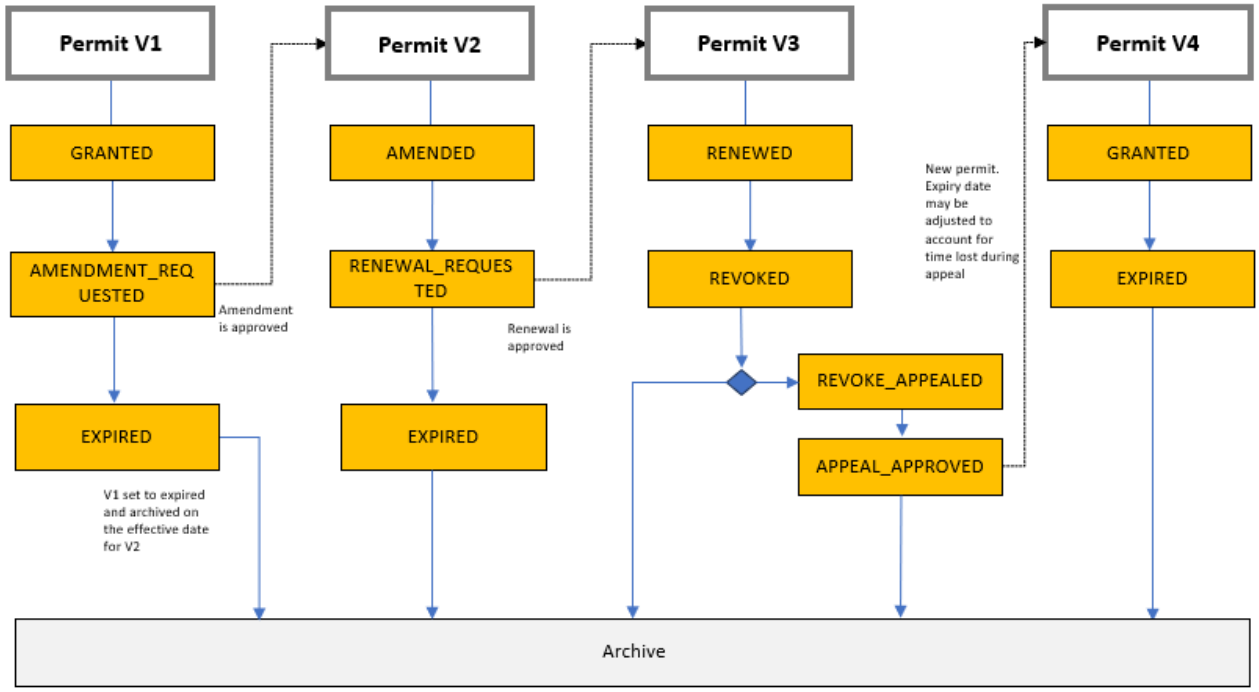
The format permit IDs is determined at national level but can follow similar logic to existing version numbering formats such as Semantic Versioning (SemVer). The MS MAY wish to adopt a common permit-numbering format to ensure each permit issued within the EHDS framework has a unique ID.

R9.3.9 DAAMS SHOULD enable the HDAB to issue amendment permits with an effective date in the future. This enables a managed transition from the existing permit to the amended permit. A transition period MAY be necessary to allow reconfiguration of the SPE to the new permit conditions, list of authorised individuals etc.

R9.3.10 Permits that issue following approval of a renewal request or a revocation appeal SHOULD issue with immediate effect and do not require a future effective date.

R9.3.11 The DAAMS MAY be configured to automatically issue alerts to HDAB personnel in advance of the expiry of a data permit.

Figure 1: Illustrative lifecycle of permit that is amended, renewed and revoked.



- Approval of Amendment request, Renewal request or Revoke appeal triggers generation of new permit version.
- Archived versions of the permit can be retrieved.
- A log of all events and status changes is created.

9.4 After a decision

Permit amendments

R9.4.1 DAAMS MUST enable the HDAB to document that a data user has applied for a permit amendment.

R9.4.2 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.

R9.4.3 DAAMS MUST enable the HDAB to document its decision to a request for amendment and to associate this with the application record.

R9.4.4 DAAMS MUST enable the HDAB to record the specific amendments approved.

Permit renewal

R9.4.5 DAAMS MUST enable the HDAB to document that a data user has applied for a permit renewal (extension of validity date of permit).

R9.4.6 DAAMS MAY be configured to enable requests for permit renewal 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.

R9.4.7 DAAMS MUST enable the HDAB to document its decision to a request for renewal and to associate this with the application record.

R9.4.8 DAAMS MUST limit permit renewal to one renewal per permit.

Permit revocation

R9.4.9 DAAMS MUST enable the HDAB to set a permit status to REVOKED.

R9.4.10 DAAMS MUST enable the HDAB to document its justification for revocation and to link this to the application record.

R9.4.11 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.

R9.4.12 DAAMS MAY be configured to enable revocation appeals to be submitted directly to DAAMS. Otherwise, DAAMS must enable the justification provided by the data user for an appeal to be stored and linked to the application record.

R9.4.13 DAAMS MUST enable the HDAB to document the decision on a revocation appeal and to associate this with the application record.

10 Processing decision appeals for application

R10.0.1 Member States MUST create national procedures enabling data applicants to appeal decisions.

R10.0.2 The ability to appeal applies to both health data access applications and health data requests.

R10.0.3 DAAMS MUST enable the HDAB to provide information on appeal mechanisms, either in the decision message or via the user interface or both.

R10.0.4 The appeal mechanism MAY be integrated into DAAMS as a workflow or be conducted through other channels such as email or in writing.

R10.0.5 DAAMS MUST enable all documentation and correspondence relating to a decision appeal to be saved and associated with the application record, where appeals are not fully integrated into DAAMS.

R10.0.6 DAAMS MUST enable the formal, signed decision on an appeal (e.g. PDF) to be saved and linked with the application record.

R10.0.7 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.

11 Fetching related data permits for mutual recognition

R11.0.1 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

The EHDS Regulation calls for a simplified assessment procedure where a trusted data holder (TDH) is involved in the evaluation of applications. The DAAMS MAY support the participation of TDH during the assessment phase. The involvement of a TDH does not affect the HDAB's legal responsibility for the final decision.

R12.0.1 DAAMS MAY support TDH involvement either through a GUI or through APIs enabling integration with external systems.

R12.0.2 Where DAAMS provides support to TDH via a GUI , the system MUST:

- Enable a visual and structured assessment workflow.
- Support the transfer of applications to, or provide controlled access to applications for, TDH for assessment purposes.
- Enable TDH to view active applications and requests that have been formally referred to them.
- Enable TDH to record their assessment of a health data access application or a health data request against the applicable criteria laid down in Article 68(1) and (2) or Article 69(2) and (3) of the EHDS Regulation.
- Enable TDH to submit their assessment to the HDAB, including a proposal for decision.
- Enable the HDAB to review the proposal and formally accept or reject the TDH's proposed decision.

R12.0.3 Additionally, DAAMS SHOULD:

- Enable the HDAB to document the rationale for accepting or rejecting the TDH's proposal.

Enable documenting of the decisions taken by the HDAB, along with the rationale behind those decisions.

System functionality supporting TDH involvement does not modify the allocation of responsibilities under the EHDS Regulation. The HDAB retains exclusive competence for *determining the conditions for data access in accordance with articles 68(10)* and for issuing the formal decision on the data application.

13 Interaction with secure processing environments

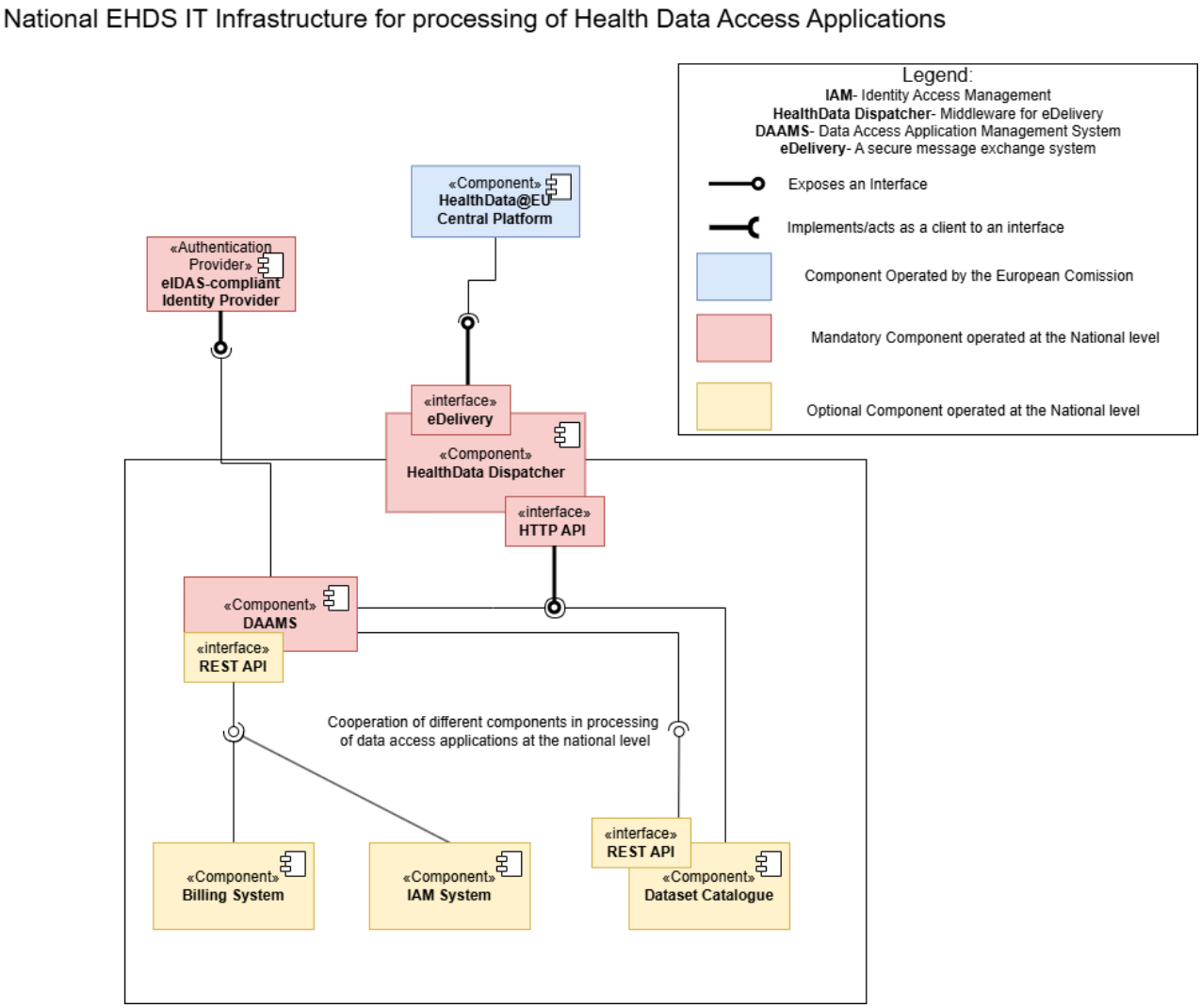
Secure processing environments (SPEs) are outside the operational scope of this specification. The functional, operational, security and interoperability requirements applicable to SPEs are defined separately in the TEHDAS2 deliverable 7.4 on SPEs. In particular, SPE-related operations such as environment creation, data reception, data upload, data analysis, results extraction, and environment decommissioning are specified there and are not further defined in this document.

R13.0.1 DAAMS MUST support the handover, or structured availability, of the permit information needed by the designated SPE or SPE operator to configure access and processing in accordance with the valid data permit. At a minimum, this SHALL include the permit identifier and version, the authorised natural persons or their identifiers, the permit validity period, and any amendment, renewal, revocation or other change affecting the validity or conditions of the permit.

R13.0.2 DAAMS MUST support recording or communication of the key lifecycle events necessary to maintain an auditable link between the application, the permit and the designated SPE. This does not imply that DAAMS implements SPE operational workflows. Detailed interface definitions, message schemas and technical protocols for SPE interaction are outside the scope of this specification and SHALL be defined in the relevant external technical documentation and SPE specifications.

14 DAAMS within national EHDS IT infrastructure for secondary usage of health data

Figure 2: Example national EHDS IT Infrastructure for processing of Health Data Access Applications



The processing of applications incoming from the HealthData@EU Central Platform is illustrated in the message sequence diagram in Figure 5. The interaction involves three components: the HealthData@EU Central Platform, the HealthData Dispatcher (a communication gateway of the national contact point, and the national DAAMS instance.

R14.0.1 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.

R14.0.2 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 IT Infrastructures for processing of Health Data Access Applications.

R14.0.3 Communication between DAAMS and HealthData Dispatcher MUST be secure, encrypted in transit using TLS version 1.2 or higher, and verified regularly to ensure availability and integrity. The system SHOULD implement monitoring and alerting for NCP communication failures, message delivery delays, or other anomalies, ensuring timely resolution and reporting.

R14.0.4 DAAMS MUST be able to queue, retry, or at least log failed exchanges to prevent data loss and to maintain an auditable trail of all interactions with the EU dispatcher. The system SHOULD provide dashboards or metrics for administrators to monitor message throughput, success rates, and system latency for cross-border requests.

R14.0.5 DAAMS MUST undergo interoperability testing with the national contact point prior to integration with the HealthData@EU infrastructure. These tests are required to validate end-to-end message exchange, including submission and retrieval of applications, response handling, error processing, and security mechanisms such as TLS/HTTPS and eIDAS-based authentication. The purpose of these tests is to ensure that DAAMS operates correctly and reliably in conjunction with the NCP and is capable of interoperating with the HealthData@EU Central Platform. While the HealthData@EU Test Framework [3]provides guidance for testing between the Central Platform and each NCP, it does not cover NCP–DAAMS interactions; therefore, a separate validation of DAAMS–NCP interoperability is required before deployment.

The sequence of messages between HealthData@EU Central Platform – NCP - DAAMS 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 health data access application or health data request to the national contact point 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

[3] https://op.europa.eu/s/AcMJ

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.

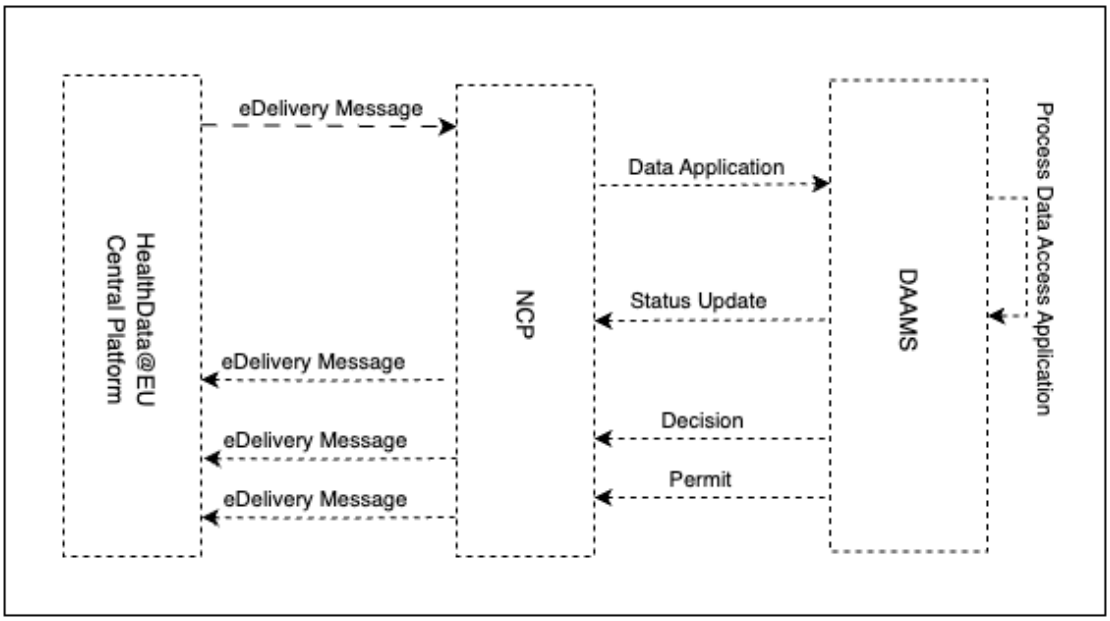
NCP then forwards this decision to the HealthData@EU Central Platform

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 3: Message sequence diagram depicting the communication between DAAMS, NCP and HealthData@EU Central Platform. Note that not all messages are illustrated.



For a complete OpenAPI description of the HealthData@EU Dispatcher, refer to the Release 6 documentation[4] and the OpenAPI specification of the National Dispatcher[5]. This documentation provides detailed definitions of the available endpoints, request and response formats, authentication and authorisation mechanisms, supported message types, and error handling procedures.

15 Non-functional requirements

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

R15.0.1 DAAMS SHOULD be designed and implemented in alignment with the principles of the European Interoperability Framework (EIF) [6]to support interoperable, user-centric, and cross-border digital public services.

15.1 Time zone / Timestamps

R15.1.1 All system-generated timestamps MUST be recorded in Coordinated Universal Time (UTC) and expressed using the ISO 8601 extended format (e.g. 2025-05-19T14:23:00Z).

[4] https://op.europa.eu/s/AcMI
[5] https://health-data-national-dispatcher.acceptance.data.health.europa.eu/
[6] https://ec.europa.eu/isa2/eif_en/

R15.1.2 Timestamps SHOULD be recorded with a precision of at least milliseconds where supported by the underlying platform.

R15.1.3 Timestamps MUST include date, time, and time zone offset or the Z (Zulu) suffix for UTC.

R15.1.4 The system MAY display local time to users for convenience but MUST store and exchange all timestamps in UTC.

R15.1.5 All logs, application lifecycle events, permit records, and status updates exchanged via APIs MUST use UTC timestamps to ensure consistency across Member States.

R15.1.6 Where applicable, the system SHOULD synchronise its internal clock using NTP (Network Time Protocol) with a reliable time source.

15.2 Graphical user interface

R15.2.1 The system MUST provide a graphical user interface (GUI) accessible to authorised users, including HDAB personnel and other relevant roles involved in the data access workflow.

R15.2.2 The GUI MUST enforce role-based access control (RBAC), ensuring that users can only view and perform actions that are permitted by their assigned roles.

R15.2.3 The GUI MUST present functionality, data, and workflow steps in accordance with the user's permissions, and MUST NOT expose unauthorised information or actions.

R15.2.4 The GUI MUST comply with accessibility standards based on EN 301 549 and WCAG 2.1 Level AA[7] (or later harmonised version) for all interactive user interface components and workflows.

R15.2.5 The GUI SHOULD follow established usability and user experience principles such as consistent navigation, visible focus indicators, clear feedback, and support for keyboard and assistive technologies.

R15.2.6 The GUI MUST support the latest two major versions of modern desktop browsers (e.g., Chrome, Firefox, Edge, Safari). Mobile browsers SHOULD be supported for the adapted subset of functionality.

15.3 System load

R15.3.1 DAAMS MUST be capable of handling concurrent access requests and data processing operations proportional to the size of the published dataset catalogue.

Let D denote the number of datasets published in the catalogue. DAAMS SHOULD support at least $U = \max(50, 5 \times \sqrt{D})$ concurrent access requests without unacceptable performance degradation. Under normal load conditions (up to U concurrent requests), DAAMS SHOULD ensure that 95% of requests complete within ≤ 2 seconds and 99%

[7] https://www.w3.org/TR/WCAG21/

within ≤ 5 seconds. Under peak load conditions (up to 2 × U concurrent requests), DAAMS SHOULD ensure that 95% of requests complete within ≤ 5 seconds.

Performance degradation with respect to the number of published datasets SHOULD NOT exceed logarithmic complexity (O(log D)) for catalogue queries and access-control operations.

R15.3.2 DAAMS SHOULD support load balancing and dynamic resource scaling to maintain responsiveness under varying load conditions.

R15.3.3 DAAMS SHOULD achieve a minimum service availability of 99.5% per calendar month, excluding planned maintenance windows, and MUST degrade gracefully under overload conditions.

R15.3.4 DAAMS SHOULD remain usable under low bandwidth and high latency conditions.

15.4 Auditing

R15.4.1 DAAMS MUST provide a secure, verifiable, and tamper-evident record of all actions affecting applications and permit issuance, ensuring transparency, accountability, and compliance with applicable legal and business requirements.

R15.4.2 DAAMS MUST log the following information for each auditable event:

- Actor identity (user ID and role)
- Action performed
- Target resource (dataset, request, permit)
- Date and time of action (UTC, ISO 8601)
- Context or outcome of the action (e.g., decision status, changes applied)

R15.4.3 Audit logs MUST be immutable, tamper-evident, and accessible only to authorised personnel. Logs MUST be retained for a minimum period of X years (as required by applicable national law) and MUST be protected against unauthorised deletion or modification.

R15.4.4 The auditing SHOULD cover, but is not limited to, the following events:

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

R15.4.5 The system SHOULD support cryptographic verification of log integrity and MAY provide exportable audit logs for external review or regulatory inspection.

R15.4.6 DAAMS MUST implement continuous monitoring based on logged events to support multiple aspects of system operation. Security monitoring MUST detect suspicious activity, unauthorised access attempts, and anomalies in system behavior, triggering formal incident response procedures. Operational monitoring MUST track system health, including CPU, memory, disk usage, network performance, API responsiveness, and service uptime, ensuring DAAMS meets performance, availability, and reliability requirements. Business monitoring SHOULD provide metrics and alerts on workflow processes, such as submitted applications, pending approvals, permit issuance times, and SLA compliance, enabling management and HDAB personnel to oversee operations effectively.

R15.4.7 Alerts generated by security or operational monitoring MUST trigger defined incident response procedures. Incident response processes MUST include containment, mitigation, investigation, reporting, and remediation, in accordance with applicable EU and national regulations. Security and operational incidents MUST be logged in a tamper-evident manner and reviewed regularly by authorised personnel.

R15.4.8 Audit logging and monitoring mechanisms SHOULD align with relevant EU cybersecurity and digital service guidance, including:

- ENISA technical guidance under the NIS2 Directive[8], for secure, resilient, and auditable logging of critical digital services.
- Auditability principles from the European Interoperability Framework (EIF), ensuring traceable and verifiable activity records across Member States.
- Sectoral legislation where applicable (e.g., AI Act), mandating comprehensive event logging for compliance and accountability.

15.5 Authentication and authorisation management

R15.5.1 DAAMS MUST be protected against unauthorised access and MUST implement secure authentication and authorisation mechanisms appropriate for the submission and processing of health data access applications and health data requests for secondary use.

R15.5.2 DAAMS MUST authenticate natural persons and legal entities using an eIDAS-compliant electronic identification and authentication provider.

R15.5.3 DAAMS MUST implement internal authorisation mechanisms to manage permissions for HDAB personnel and other authorised users. This includes:

- Enforcing role-based access control (RBAC) for all workflows and actions
- Ensuring users can only perform operations and access data aligned with their assigned roles
- Logging unauthorised access attempts and enforcing session control for sensitive actions

[8] http://data.europa.eu/eli/dir/2022/2555/oj

R15.5.4 Authorisation decisions MUST be enforced at the DAAMS application level and MUST NOT rely solely on the eIDAS authentication provider.

R15.5.5 The system MUST ensure that all authorisation rules comply with applicable national legislation and internal HDAB procedures.

15.6 Application programming interface

R15.6.1 DAAMS SHOULD expose an API to allow authorised users and systems to interact with DAAMS functionality.

The API implementation is under the control of the Member State. Member States MAY choose any architecture, framework, or internal design that meets national requirements.

R15.6.2 All cross-border communication MUST be conducted via the national healthdata@eu dispatcher, ensuring interoperability with the Central Platform through the NCP using the standardised EU interfaces.

R15.6.3 The API SHOULD use widely adopted web standards such as REST over HTTPS with JSON payloads to ensure security, maintainability, and ease of integration.

R15.6.4 The system MUST enforce authentication and authorisation for all API access, consistent with DAAMS user management and eIDAS-compliant identity verification.

R15.6.5 API responses MUST include standardised error handling, clear status codes, and timestamps in UTC (ISO 8601) format, in alignment with EHDS data exchange requirements.

15.7 Support and training

R15.7.1 DAAMS MUST provide comprehensive user training for all authorised personnel, including HDAB personnel and other roles involved in data access workflows. Training MUST cover system usage, role-based access procedures, data protection responsibilities, audit logging interpretation, incident reporting, and security best practices.

R15.7.2 DAAMS MUST provide easily accessible user support resources, including user manuals, contextual help within the GUI, FAQs, and contact points for technical and operational assistance. Support MUST be available for both routine inquiries and urgent issues affecting applications or system operations.

R15.7.3 DAAMS SHOULD provide role-specific training and refresher sessions to ensure that personnel are up to date with system updates, new features, or changes in national and EU regulations affecting data access workflows.

R15.7.4 The system SHOULD include mechanisms for reporting issues directly from the GUI or API, with workflow tracking to ensure timely resolution and follow-up.

16 Security considerations

R16.0.1 DAAMS MUST implement mitigations for common security threats in accordance with the latest OWASP Top 10 [9]guidance. Implementers MUST regularly review the current OWASP Top 10 publication and apply recommended countermeasures for risks such as injection, broken authentication, broken access control, security misconfigurations, cross-site scripting, and insecure deserialisation.

R16.0.2 All communication between clients, APIs, and the DAAMS backend MUST be encrypted in transit using TLS version 1.2 or higher with strong, modern cipher suites. TLS MUST NOT be downgraded to insecure protocols such as SSL 2.0/3.0 or TLS versions below 1.2, and TLS 1.3 is strongly recommended where supported. Certificates MUST be valid, signed by a trusted certificate authority, and configured according to modern best practices, including appropriate key lengths and expiration periods.

R16.0.3 DAAMS SHOULD undergo independent TLS configuration testing using SSL Labs or an equivalent public/industry-recognised tool. The system SHOULD achieve an A grade or higher to demonstrate secure protocol configuration, strong cipher suites, proper certificate management, and absence of known TLS vulnerabilities. TLS testing MUST be repeated periodically, such as after major updates or certificate renewal, to ensure continued compliance.

R16.0.4 Sensitive data stored within DAAMS MUST be encrypted at rest using industry-standard encryption algorithms (e.g., AES-256). Key management MUST follow security best practices to protect confidentiality and integrity.

R16.0.5 DAAMS MUST implement additional security best practices, including secure session management with timeout policies, input validation and output encoding to prevent injection attacks, and the principle of least privilege for all system components. Regular vulnerability assessments and patching procedures MUST be in place to maintain security over time.

17 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.

[9] https://owasp.org/www-project-top-ten/

18 Annexes

Annex number	Annex title
1	Methodology
2	Public consultation summary
3	User journey
4	Glossary

Annex 1 – Methodology

This technical specification for DAAMS was developed through a structured regulatory and technical analysis process. The primary foundation of the work was a detailed review of the European Health Data Space (EHDS) Regulation, ensuring that all requirements are aligned with the legal provisions concerning secure processing, interoperability, governance of access, and cross-border data exchange. This legal analysis was complemented by a review of publicly available HealthData@EU technical releases and related documentation to ensure consistency with EU-defined APIs, messaging standards, and operational workflows. In addition, relevant EU-level guidance, including the European Interoperability Framework (EIF) and ENISA cybersecurity recommendations, was considered to ensure alignment with established interoperability and security principles.

The analysis also drew on practical experience from previous initiatives, including the EHDS pilot and the first TEHDAS joint action. Lessons learned from these activities informed the specification in areas such as authentication, authorisation, audit logging, monitoring, and secure data exchange. The findings from regulatory analysis, technical documentation review, and project evaluations were synthesised into a coherent set of functional and non-functional requirements. Where appropriate, requirements are traceable to specific EHDS provisions or HealthData@EU documentation. This specification does not redefine technical standards already established at EU level but references relevant Commission documentation where detailed technical implementation guidance is required.

The deliverable underwent a structured review process within the TEHDAS2 joint action. It was subject to internal consortium review prior to public consultation to ensure technical accuracy and consistency. Following this, the draft was opened to a public consultation, allowing stakeholders to provide feedback and propose improvements. The revised version incorporates relevant feedback received through this process. In addition, the specification was discussed and refined through consultations with DG SANTE and must be formally accepted by the TEHDAS2 project steering group (PSG) prior to final publication.

All requirement statements in this specification follow RFC 2119 terminology (MUST, MUST NOT, SHOULD, SHOULD NOT, MAY). Items marked as MUST define mandatory system capabilities necessary to ensure compliance with the applicable regulatory framework and represent the core functional requirements of DAAMS. Items marked as SHOULD or MAY indicate recommended or optional capabilities that enhance usability, security, interoperability, or operational efficiency but are not strictly required for baseline compliance.

Annex 2 – Public consultation summary

A draft version of this document was in public consultation in October-November 2025. This document was commented in total for 45 times. The number of responses may contain some duplicates as there was no individual identification and verification required to respond to the surveys. Some respondents have also responded both from data holder's and data user's perspective. The responses came from 18 different countries from the EU countries and the European Economic Area countries. Responses from Eastern and Southern European countries and international organisations were largely missing. The respondents were primarily from three main types of organisations, listed in order of prevalence: public organisations, academic/research organisations, and private organisations.

The public consultation on deliverable 6.4 – DAAMS Specification generated constructive and detailed feedback from multiple stakeholders. Overall, respondents acknowledged that the document is well structured and that the requirements are clearly formulated. However, several comments highlighted the need for improved clarity, consistency, and traceability. In particular, stakeholders requested clearer distinction and numbering of requirements, more consistent use of normative language (MUST/SHOULD/MAY), better alignment of terminology, and removal of duplications or ambiguities across chapters and figures.

A recurring theme in the feedback was the need to strengthen interoperability, traceability, and implementation clarity, while avoiding over-specification of technical details. Several respondents suggested clearer references to existing Commission and HealthData@EU documentation for technical standards, security requirements, accessibility, and message formats. Other comments focused on improving lifecycle descriptions, clarifying roles and responsibilities, ensuring consistency between diagrams and text, and enhancing non-functional requirements such as accessibility and auditability.

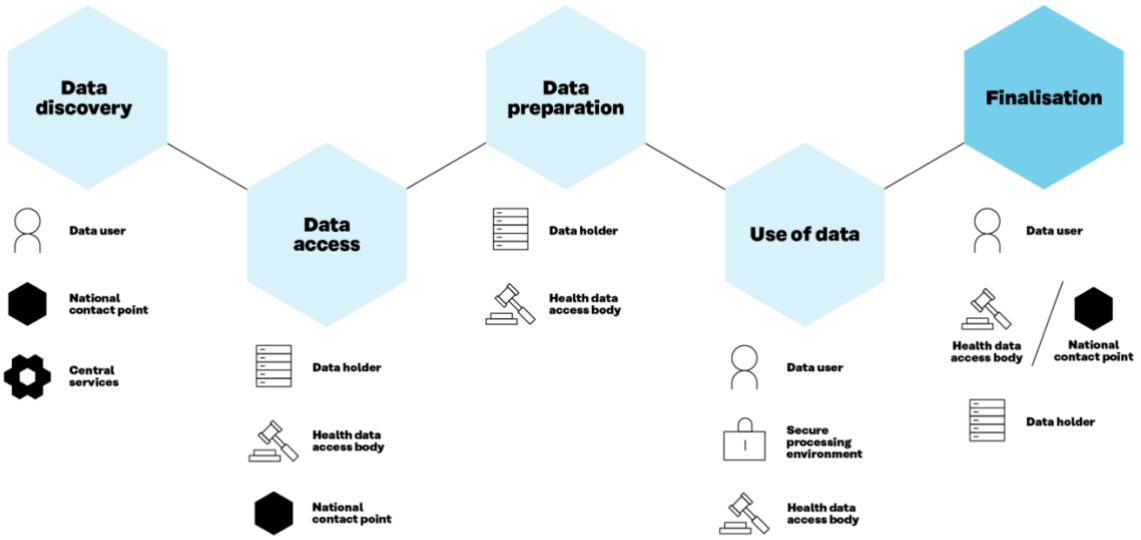
The revised version of the document takes these comments into account, either through structural improvements and clarifications within scope or by explicitly referencing the relevant Commission documentation where technical completeness is required.

Annex 3 – 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 environment. The duration of this phase is specified in the regulation (Art 68(12)).

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

Annex 4 – Glossary

Project partners have added key terms and their definitions used in the milestones and deliverables to this glossary. The aim is to ensure harmonised terminology in all the TEHDAS2 deliverables.

This is a copy from a living document to be updated throughout the joint action. This version is from 27 February 2026.

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).
AI system	A machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual

	environments. AI Act – Regulation (EU) 2024/1689, Article 3(1)
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	Where applicable, 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. Aggregation is one possible anonymisation technique.
Applications	For the purposes of this document, health data access applications and health data requests.
Areas of occupational health	Areas of occupational health are the main disciplines concerned with protecting and promoting works health

	and safety in the workplace. It includes: - Occupational medicines: Prevention and management of work-related diseases, - Occupational hygiene: Identification and control of workplace hazards - Occupational safety: Prevention of accidents and injuries - Occupational health nursing: Workplace health services - Ergonomics: adapting work to fit the worker - Occupational psycology: Mental health and well-being at work - environmental healt: Control of enviornmental risks affecting workers A case of occupational disease is defined as a case recognised by the national authorities responsible for recognition of occupational diseases. The data shall be collected for incident occupational diseases and deaths due to occupational disease. Work-related health problems and illnesses are those health problems and illnesses which can be caused, worsened or jointly caused by working conditions. This includes physical and psychosocial health problems. A case of work-related health problem and illness does not necessarily refer to recognition by an authority and the related data shall be collected from existing population surveys such as the European health interview survey (EHIS) or other social surveys. Regulation (EU) 1338/2008, Annex V, (b) and WHO2, Article 3(c)

Areas of Public Health	'Public health' shall mean all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Regulation (EU) 2021/2282, Article 2(5).
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 or legal person listed in the data permit, giving them the rights to process sensitive data inside a secure processing environment.
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	A phase in the EHDS user journey during which the user fills in and submits a dedicated and standardised data access application form or a data request to a health data access body (HDAB). The user must complete the information required in the form, upload necessary documents, and provide justifications as needed.
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 a 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(2) point (v))
Data preparation	Data preparation is the process in which an organisation (in this case the data holder or the health data access body) 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.
Data processing	Any operation or set of operations which is performed on personal/non-personal data or on sets of personal/non-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. (Modified from the 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	Processing data respecting the principles laid down in GDPR Article 5(1). The “implementation of appropriate administrative, technical or physical means to guard against unauthorised 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 **EHDS user journey** where prepared health data is made accessible to authorised users for secondary purposes.
Data quality	Data quality means the degree to which the elements of electronic health data are suitable for their intended primary use and secondary use; (EHDS Article 2(2) point (z))
Data quality and utility label	Data quality and utility label means a graphic diagram, including a scale, describing the data quality and conditions of use of a dataset. (EHDS Article 2(2) point (aa))
Dataset	A structured collection of electronic health data. (EHDS Article 2(2) point (w))
Dataset catalogue	A collection of dataset descriptions, arranged in a systematic manner and including a user-oriented public part, in which information concerning individual dataset parameters is accessible by electronic means through an online portal. (EHDS Article 2(2) point (y)
Dataset description	A description in the form of metadata of the available datasets and their characteristics (EHDS Article (77(1))
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.
Data user application (a software linked to a 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.
Development activities	The concept 'Development activities' is not clearly defined in any legal act. However, there is a definition of the notion of research and development in Directive 2009/81/EC, Article 1(27): 'Research and development' mean all activities comprising fundamental research, applied research and experimental development, where the latter may include the realisation of technological demonstrators, i.e. devices that demonstrate the performance of a new concept or a new technology in a relevant or representative environment." Directive 2009/81/EC, Article 1(27)
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.
European Health Data Space (EHDS) user journey	The path of a data user applying for electronic health data for secondary use purposes within the European Health Data Space (EHDS). A simplified version of a EHDS user journey is included in the annexes of TEHDAS2 deliverables. It consists of five main phases: data discovery, data access, data preparation, use of data and finalisation.
Electronic health data	Personal or non-personal electronic health data (EHDS Article 2(2) point (c)).
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(2) point (y))
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

	(IT infrastructures), 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 (IT infrastructures), 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 (IT infrastructures) 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/source data**. High fidelity means that distributions, correlations, and key patterns remain unchanged.
Healthcare	'Healthcare' means health services provided by health professionals to patients to assess, maintain or restore their state of health, including the prescription, dispensation and provision of medicinal products and

	medical devices. Directive 2011/24/EU, Article 3(a)
Health data access application	An application form used to seek access for 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. (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(2) point (t))
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(2) point (u))
Health technology assessment (HTA)	A multidisciplinary process that summarises information about the medical, patient and social aspects and the economic and ethical issues related to the use of a health technology in a systematic, transparent, unbiased and robust manner. (Regulation (EU) 2021/2282 on health technology assessment and amending Directive 2011/24/EU, Article 2(5))
High performance computing (HPC)	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 (EU) No 608/2013 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(2) point (f))
Invoice	A legally binding commercial document, detailing the complete cost

	structure with breakdowns by services and data holders. It contains disaggregated cost elements.
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. If the pseudonymising transformation is truly irreversible and re-identification is no longer reasonably possible, the resulting data qualify as anonymised data rather than pseudonymised data under the GDPR.
Legal basis of data processing	The criteria defined in EHDS Regulation Article 68 for health data access bodies to assess whether an applicant can be given a permit to process electronic health data. The conditions under which personal data processing is considered lawful are laid down in GDPR, Article 6. Purposes for which the electronic health data can be processed for secondary use are laid down in EHDS Regulation, Article 53.
Medicinal product	Any substance or combination of substances presented for treating or preventing disease in human beings. Any substance or combination of substances which may be administered to human beings with a view to making a medical diagnosis or to restoring, correcting or modifying physiological functions in human beings is likewise considered a medicinal product. Directive

	2011/24/EU referring to Directive 2001/83/EC, Article 1(2)
Medical device	Any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes: • diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease • diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability • investigation, replacement or modification of the anatomy or of a physiological or pathological process or state • providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations, and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means. The following products shall also be deemed to be medical devices: • devices for the control or support of conception • products specifically intended for the cleaning, disinfection or sterilisation of devices as referred to in Article 1(4) and of those referred to in the first paragraph of this point.

	Regulation (EU) 2017/745 and (EU) 2017/746, Article 2(1)
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. (Directive (EU) 2019/1024 on open data, “Open Data Directive”)
Open (data) database	Publicly accessible digital data that anyone can freely use, reuse, and redistribute for any purpose.
Original/source 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.
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.
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.
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 sector body	'Public sector body' means the state, regional or local authorities, bodies governed by public law, or associations formed by one or several such authorities or one or several such bodies governed by public law." Regulation (EU) 2022/868, Data Governance Act, Article 2(17).
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**. To add a source
Public value (of data use)	For analytical or policy discussion purposes, public value could be understood as 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.
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.
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(2) point (e))
Secure processing environment (SPE)	An environment in which access to electronic health data can be provided in following a data permit. A secure processing environment 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)).
Serious cross-border threats	This Regulation shall apply to public health measures in relation to the following categories of serious cross-border threats to health: (a) threats of biological origin, consisting of: (i) communicable diseases, including those of zoonotic origin; (ii) antimicrobial resistance and healthcare-associated infections related to communicable diseases ('related special health issues'); (iii) biotoxins or other harmful biological agents not related to communicable diseases; (b) threats of chemical origin; (c) threats of environmental origin, including those due to the climate; (d) threats of unknown origin; and (e) events which may constitute public health emergencies of international concern under the International Health Regulations (IHR) ('public health emergencies of international concern'), provided that they fall under one of the categories of threats set out in (a–d) Regulation (EU) 2022/2371, Article 2(1)

Statistics	Quantitative and qualitative, aggregated and representative information characterising a collective phenomenon in a considered population. Regulation (EU) 223/2009, Article 3(1)
Synthetic data	Artificially generated data. 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	Transfer of data outside of the European Union or European Economic Area according to the three cumulative criteria identified by the European Data Protection Board (EDPB): • ”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)	A research environment that aims 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. TREs emerged from the UK health research sector, shaped by community-led principles and structured around flexible, function-based zones.
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)
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**.