European Health Data Space for Secondary Use @CY - CY-EHDS-2ND

Proposal number: 101129405

D5.1 DAAMs Requirements, Specifications and Prototype

(Co-)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.

Author(s)

Name	Surname	Country	Organisation	Role of the Organisation
Nicoletta	Prentza	Cyprus	University of Cyprus (UCY)	Affiliated Entity (AE)
Maria	Papaioannou	Cyprus	UCY	AE
Ioannis	Rodosthenous	Cyprus	UCY	AE
Constantinos	Pattichis	Cyprus	UCY	AE

Reviewed by

Name	Surname	Country	Organisation	Role of the Organisation
Christos	Schizas	Cyprus	NeHA	Competent Authority (CA)
Ioannis	Konstantinou	Cyprus	UCY	AE
Antonis	Stylianides	Cyprus	NeHA	CA
Theodoros	Kyprianou	Cyprus	NeHA	CA

Abbreviations

AE	Affiliated Entity
CA	Competent Authority
CP	Central Platform
CPL	Central Platform Layer
CY-EHDS-2nd	European Health Data Space for Secondary Use @CY
CY-HDAB	Health Data Access Body of Cyprus
CY-HDAB-2nd	Health Data Access Body of Cyprus for secondary use of health data
DAAMs	Data Access Application Management solution
EC	European Commission
EHDS	European Health Data Space
eIDAS	Identification, Authentication and Trust Services (eIDAS)
EU	European Union
HDAB	Health Data Access Body
ESPE	External Secure Processing Environment
IAA	Identification, Authentication and Authorization
ISPE	Internal Secure Processing Environment
NCP	National Contact Point
NeHA	Ethniki Archi Ilektronikis Igeias – National eHealth Authority
NFR	Non-Functional Requirements
nHDsC	National Dataset Catalogue for health data
SPE	Secure Processing Environment
TEHDAS2	Second Joint Action Towards the European Health Data Space
UCY	University of Cyprus
WP	Work Package

Executive Summary

The Data Access Application Management solution (DAAMs) is one of the core modules of the CY-EHDS-2nd[1] Central Platform (CP). The system is 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 (EU) 2025/327[2]. Its primary role is to process health data access applications and health data requests for secondary uses, such as research, innovation, policymaking and other purposes listed in Art. 53 EHDS.

The scope of this deliverable is to specify the requirements for the Health Data Access Body of Cyprus (CY-HDAB) National eHealth Authority (NeHA) to develop and deploy the DAAMs module. It includes use cases, functional requirements, business logic and some considerations about the technical solution. This work built upon the outputs of the Analysis & Design of HealthData@EU CP[3] infrastructure, as well as the Second Joint Action Towards the European Health Data Space (TEHDAS2)[4], to ensure alignment and interoperability with the other Health Data Access Bodies (HDABs). Any aspects not explicitly specified will be defined or revised in the upcoming deliverable D5.2 'DAAMs: Implementation and piloting.

[1] https://www.cy-ehds-2nd.eu/
[2] https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng
[3] https://acceptance.data.health.europa.eu/
[4] https://tehdas.eu/

Lits of Figures

List of Tables

1 INTRODUCTION

1.1 Guidance for Interpreting the CY-EHDS-2nd Requirements and Specifications

This guidance text is intended to help the reader navigate in a meaningful and structured manner through the first series of technical deliverables concerning the requirements and specifications of the CY-EHDS-2nd national infrastructure. It provides essential context for understanding how the various components fit together and how supporting annexes serve as shared reference points across modules. This same text is included identically at the start of each deliverable in the requirements and specifications series (D5.1 to D9.1) to ensure consistency in interpretation and approach.

This deliverable is part of a coordinated set of Requirements and Specifications documents (D5.1 to D9.1) that together define the design and implementation logic for the national infrastructure supporting the secondary use of health data in the Republic of Cyprus, under the CY-EHDS-2nd project. Each module addresses a distinct part of the infrastructure, yet all share a unified architectural foundation, legal interpretation, and design methodology.

To support this shared structure and ensure full coherence across the Work Packages, a series of five common annexes (Annex A to Annex E) has been developed. These annexes are referenced throughout this and all other deliverables and are essential for a complete and accurate understanding of the specifications that follow.

The reader is strongly advised to begin by reading Annex A of D5.1. This annex provides the architectural and conceptual entry point for understanding the CY-EHDS-2nd infrastructure and explicitly references all other annexes. Only once Annex A is read, should the reader proceed to the main content of this or any other Requirements and Specifications deliverable.

1.1.1 Annexes Applicable Across All Requirement and Specifications (deliverables D5.1-D9.1)

The following annexes provide cross-cutting foundations that support the interpretation, alignment and drafting of all CY-EHDS-2nd requirements and specifications deliverables (D5.1 to D9.1). Each annex focuses on a specific dimension of the project, from technical architecture to digital business capabilities, semantic mapping, actor roles and terminology. These annexes are shared across the series to ensure coherence, eliminate duplication and align the national infrastructure design with the HealthData@EU infrastructure model.

All annexes listed below are formally included as annexes of the D5.1 deliverable and are referenced as needed across the remaining deliverables. Each annex should be understood as integral, not supplemental, to the specification content.

1.1.1.1 Annex A – CY-EHDS-2nd Architecture and CP Infrastructure

This annex presents the overall architecture of the CY-EHDS-2nd infrastructure and introduces its main functions and capabilities. It provides a high-level vision of the system's structural design and its role within the broader EU eHealth ecosystem for secondary use. It explains how the five core components, nHDsC, DAAMs, SPE, National Connector and Quality Toolbox, are interconnected through a central coordination layer (the CP Layer, (CPL)), which ensures secure, interoperable and legally compliant access to health data for secondary use. The annex also outlines the long-term modularity and scalability of the platform, highlighting its capacity to integrate future EU deliverables, including outputs from TEHDAS2, QUANTUM, and the upcoming EHDS implementing acts.

1.1.1.2 Annex B – HDAB Digital Business Capabilities

This annex contains a structured overview of the Digital Business Capabilities (DBCs) that HDABs are expected to implement, as defined by the European Commission (EC) in the context of the EHDS. While these capabilities are not themselves regulatory, they are based on and support compliance with the EHDS Regulation and provide critical guidance for implementation planning. Each capability is listed with its code, description, interdependencies, and its applicability within CY-EHDS-2nd. These capabilities were further clarified by the EC during the 2nd EHDS2 Community of Practice General Assembly (February 2025) and are formally recorded in the EHDS2 CoP Confluence.

1.1.1.3 Annex C – Indicative Mapping to HealthData@EU CP Infrastructure

This annex provides a basic, high-level mapping between selected components of the CY-EHDS-2nd national infrastructure and the HealthData@EU CP. The mapping focuses on core modules that are most relevant for interoperability and cross-border integration. While the alignment is not exhaustive or granular, it offers a conceptual view of how Cyprus national solution reuses, adapts, or complements elements of the EU reference platform. This annex supports early-stage validation of design choices and highlights areas of future alignment and integration.

1.1.1.4 Annex D – Common Actor Definitions – CY-EHDS-2nd (v1.0)

This annex defines all functional actors involved in the implementation and operation of CY-EHDS-2nd across WPs 5 to 9. Each actor is described according to its formal role, regulatory grounding and operational scope. It is aligned with the final EHDS Regulation (EU) 2025/327, Scale-Up documentation (Dec 2024), and HealthData@EU CP deliverables (Mar 2025). To ensure consistency and avoid ambiguity, any actor referenced in this deliverable must correspond exactly to the naming and definition in this annex. Updates or additions to actor roles must be formally proposed and approved at the project level.

1.1.1.5 Annex E – CY-EHDS-2nd Key Terminology

Annex E provides a project-wide glossary of terms used in D5.1 to D9.1. Each term is defined based on its actual use across the deliverables, and its meaning is aligned with the HealthData@EU CP documentation, TEHDAS2 outputs (up to May 2025), and the EHDS Regulation (EU) 2025/913. This glossary ensures conceptual clarity and harmonised understanding of terminology across the entire CY-EHDS-2nd national implementation effort.

1.1.2 Recommended Reading Order

To ensure a coherent understanding of the CY-EHDS-2nd architecture and its module-specific implementations, the following reading order is recommended:

1. D5.1 – Annex A: CY-EHDS-2nd Architecture and CP Infrastructure **(mandatory starting point)**
2. D5.1 – All other annexes, especially Annex D: Common Actor Definitions – CY-EHDS-2nd (v1.0)
3. D5.1 – DAAMs Requirements, Specifications and Prototype
4. D6.1 – nHDsC Requirements and Specifications
5. D9.1 – Health Data Quality Enhancement ToolboxRequirements and Specifications
6. D7.1 – SPE: Requirements and Specifications
7. D8.1 – National Connector for Cross-border gateway Requirements and Specifications

1.2 D5.1 Introduction

The purpose of this document is to define the requirements and specifications for the DAAMs, that will be designed and deployed as a core module of the CY-HDAB-2nd CP. DAAMs objective is to enable the Health

Data Access Body (HDAB) of Cyprus to receive, process and reply to data access and data request applications for the National Dataset Catalogue for health data (nHDsC).

1.3 CY-HDAB-2nd CP & DAAMs

The DAAM system will allow data users (applicants) to submit, track and manage data access and data request applications, for datasets available at the National Catalogue shown in **Error! Reference source not found.**. It will also allow authorized HDAB users to assess, approve or reject and issue data permits (if applicable). The DAAMs will leverage the infrastructure and services of the Health Data Access Body of Cyprus (CY-HDAB) portal such as the user management, authentication and authorization. Moreover, the DAAMs will assess, decide and communicate decisions of data access and data request applications received from the HealthData@EU CP via the National Contact Point (NCP).

1.4 Interdependencies

- CY-EHDS-2nd Architecture and CP Infrastructure (ANNEX A).
- CY-EHDS-2nd WP6: National Health Data Catalogue (*D6.1 nHDsC Requirements and Specifications*).
- CY-EHDS-2nd WP7: Secure Processing Environment (*D7.1 SPE: Requirements and Specifications*).
- CY-EHDS-2nd WP8: National Connector & Cross-border Gateway (*D8.1 National Connector for Cross-border gateway Requirements and Specifications*).
- Transparency Portal: will be implemented in the future (out-of-scope of CY-EHDS-2nd Grant).

1.5 Overview

The rest of this deliverable is organized as follows:

- Section 1: Introduction
- Section 2: DAAMS Overview
- Section 3: Requirements
- Section 4: Specifications
- Section 5: Prototype
- Section 6: References

1.6 Alignment with HealthData@EU CP

Cyprus, through the CY-EHDS-2nd grant agreement, is establishing its national infrastructure for the secondary use of health data entirely from scratch. Given the absence of an existing national framework, the project's strategic approach is to align fully with the HealthData@EU infrastructure and the CP model developed by the EC.

To achieve this, for the DAAMs component of the CY-EHDS-2nd CP:

- Adopts the HDAB DBCs blueprint.
- Bases where applicable its business requirements and technical specifications on the
  - HealthData@EU Central Services Release 3 deliverables [1-2].
  - ANALYSIS & DESIGN of HealthData@EU Infrastructure deliverables [3-7].
- Intends to adapt the European solution as fully as possible, thereby avoiding duplication of design efforts and ensuring regulatory and technical consistency.

The Analysis & Design Deliverables and Release 3 documentation has proven highly suitable to the needs and constraints of DAAMs. As a result, they will play a vital role in guiding both the drafting and refinement of national business requirements, not only during the design phase but also during pilot implementation, which will serve to validate interoperability with the EU infrastructure and prepare for subsequent CP releases.

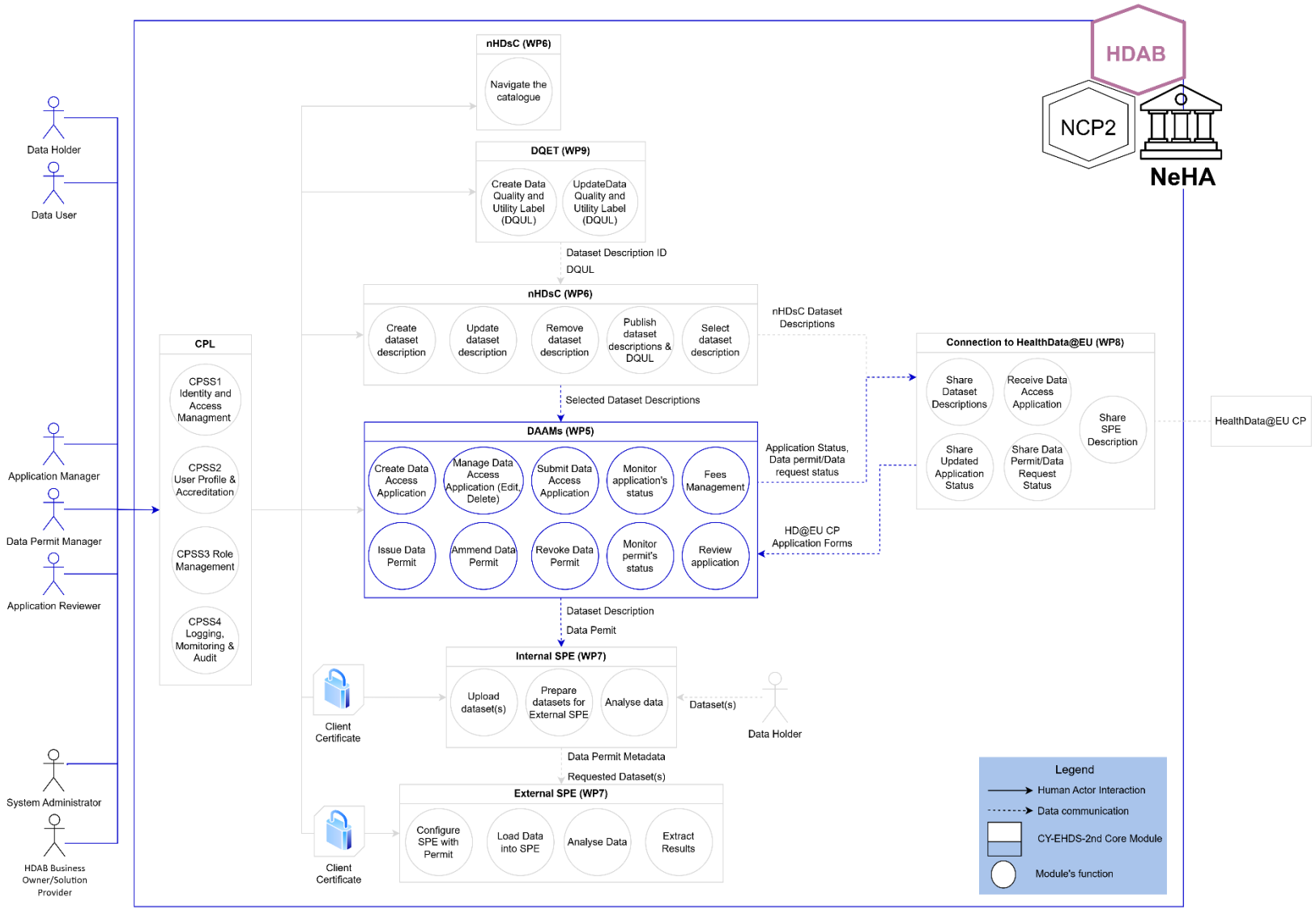

Figure 1: CY-EHDS-2nd DAAMs module (as implemented by WP5)

2 DAAMS OVERVIEW

2.1 Overview

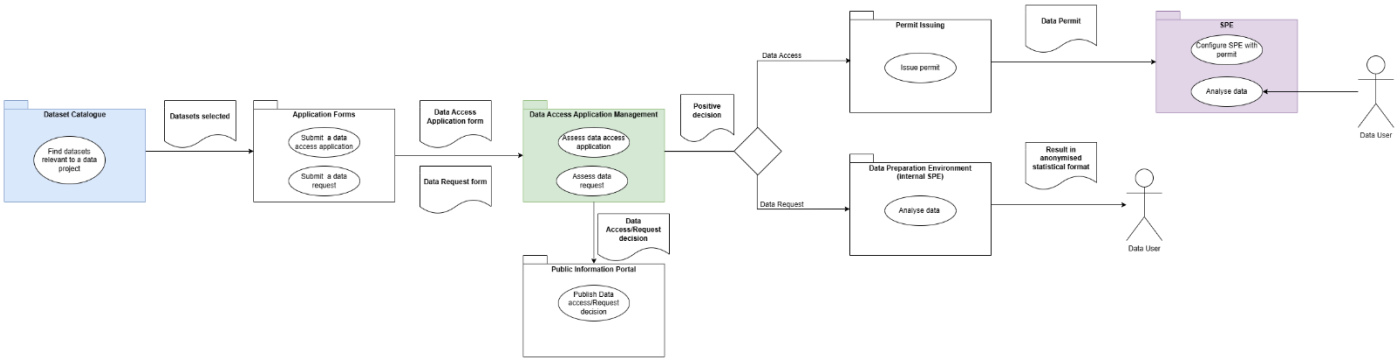

Figure 2: DAAMs overview. Diagram from the HDABs-CoP.

The DAAM system will provide functionality to support the workflow in Figure 2, from Dataset selection to Data Permit Issuing. The system is responsible for managing health data access and request applications at both national and cross-border levels. The data analysis / preparation and SPE related processes that follow a positive decision are described in the CY-EHDS-2nd D7.1 'SPE Requirements and Specifications'.

The general process supported by the DAAMs includes the following steps:

1. Completion and submission of a data access or request application by the applicant, either via the national DAAMs interface (for national cases) or via the HealthData@EU CP (for cross-border cases).
2. Reception of the application by DAAMs.
3. Assessment of the application against the legal, ethical, and technical conditions defined in the EHDS Regulation [8] and relevant national legislation. This step will most of the time be done by a human.
4. Issuance of a decision by the HDAB, indicating whether access is granted or denied and under which conditions.
5. Issuance of a data permit, if applicable, formalising the authorisation and specifying conditions of use.
6. Notification of the applicant, who must be able to access the decision and data permit, either through the CP or the national DAAMs interface.

All cross-border communication will be routed through the Cross-border Gateway of the NCP using secure eDelivery channels. The communication requirements between the DAAMs and the NCP are included in this document, whereas the communication requirements between the NCP and the HealthData@EU CP are presented in the CY-EHDS-2nd D8.1 'National Connector for Cross-border gateway Requirements and Specifications'.

2.2 Actors

The complete set of actors and their responsibilities across the CY-EHDS-2nd infrastructure is defined in *D5.1 – Annex D: Common Actor Definitions – CY-EHDS-2nd (v1.0)*. That annex serves as the single authoritative

reference for roles appearing in Work Packages 5 to 9, ensuring alignment with the EHDS Regulation and the implementation scope agreed by NeHA.

Table 1 presents only the actors relevant to this module. These have been selected from the common list based on their participation in the workflows and responsibilities specific to this work package. In the functional requirements section, Actors Involved may refer to 'HDAB users' which includes all A4, A5 and A6 actors.

Table 1: CY-EHDS-2nd DAAMs Actors as defined in *D5.1 Annex D Actor Definitions – CY-EHDS-2nd (v1.0).*

Actor No.	Role
A1	General Public Citizen
A2	Data User / Data Applicant
A3	Data Holder / Trusted Data Holder
A4	Application Manager
A5	Data Permit Manager
A6	Application Reviewer

2.3 Business uses cases

2.3.1 Applications management

The DAAM system will allow data applicants to select one or more datasets, create and submit data access or request applications, as illustrated in Figure 3.

A data applicant (national user) will be able to create a data access or request application for selected datasets, save it as draft, fill in all required fields and submit the application for assessment by CY-HDAB. During the application assessment the applicant will be able to monitor the status of the application, provide additional information, if requested by the HDAB, or withdraw the application. As soon as the assessment is completed, the applicant will be able to view the decision and access the data permit.

The DAAM system will also be able to receive and assess applications submitted to the HealthData@EU CP, for the nHDsC, via the NCP. During the assessment of these cross-border applications, all communication with the data applicant will be through the NCP.

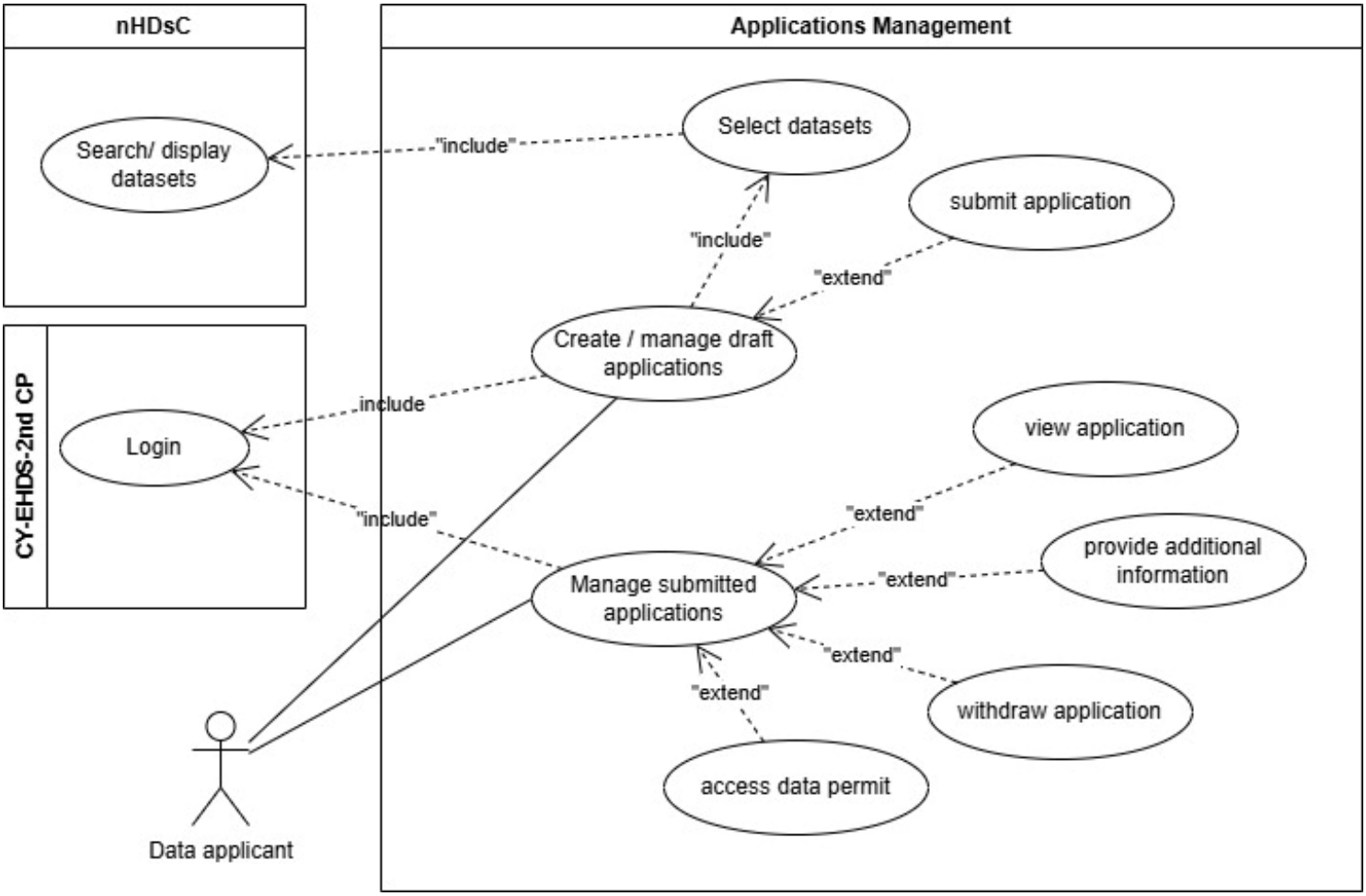

Figure 3: Applications Management Business Use case.

2.3.2 Applications assessment

The DAAM system upon receiving a data access or request application must show the application in a dedicated internal Dashboard for processing and assessment by the HDAB users. The system should offer authorized users several functions as illustrated in Figure 4.

Authorized HDAB users will be able to view the contents of the applications, publish information (for applications received at national level) (*future development*-Transparency Portal), flag applications for accelerated procedure, update application status and timelines, transfer application to a trusted data holder for evaluation – and receive their comments, request and receive additional information from the data applicant, extend the assessment period, reject or approve application, communicate the outcome of the assessment (directly to a national data applicant or via NCP to cross-border applicants).

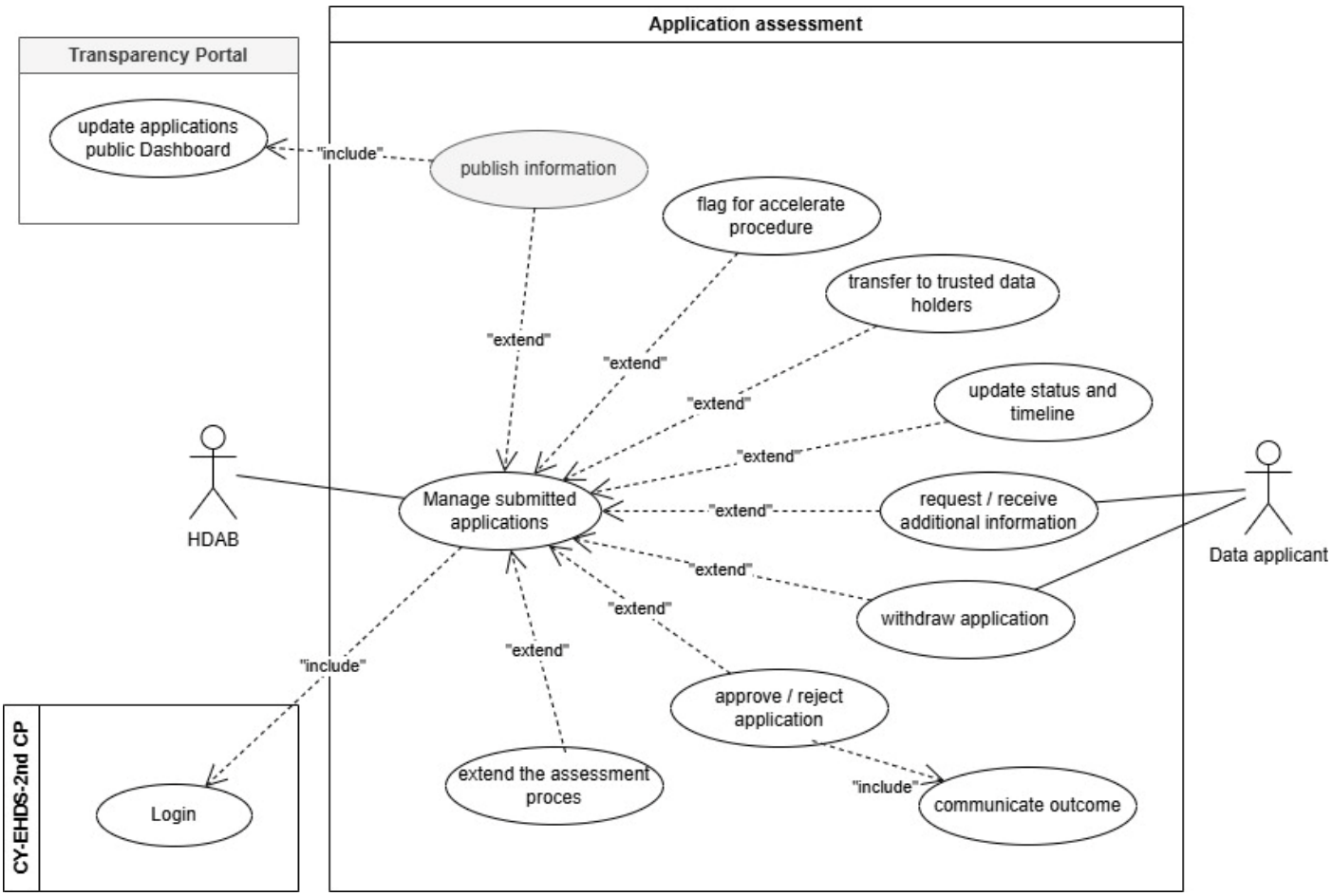

Figure 4: Applications Assessment Business Use case.
The integration with the 'Transparency Portal' will be implemented in the future (not included in the scope of this work).

2.3.3 Fees management

The DAAM system via the 'Transparency Portal' will offer a public space to clearly indicate the fee structure and may also provide a tool, such as a simulator, to estimate fees. Additionally, the system should dynamically estimate the accurate cost of data access applications and request forms based on the inputted information, informing the data applicant of the estimated fees before the submission of the form.

The system may support the generation of detailed invoices with fee breakdowns and allow applicants to pay these invoices within the system. It should support secure payment gateways and multiple payment methods, maintaining a comprehensive log of all fee-related transactions to ensure accountability and ease of auditing.

Additionally, the system may allow the negotiation of fees and provide features for adjusting application fees based on the negotiation outcome. The system should ensure timely communication with the data applicant regarding fees to avoid non-compliance and potential fines.

2.3.4 Data Permits management

Once the assessment of a data access or request application is completed, authorized HDAB users will be able to issue a document with the decision, using the "Data Permit" template (TEHDAS2 D6.3 Data permit template [9]). The data permit will include any necessary annexes that outline the terms and conditions for data access and use (including the SPE where the data processing will occur).

The system should provide functionality for reviewing and finalizing the data permit and notifying the data applicant through an integrated communication feature (for cross-border applications the system will push the notification to the NCP).

The system will provide functionality to track the permit's status throughout its lifecycle, providing updates on approvals, amendments, and impending expirations. Users will receive automatic notifications when a permit is approaching its expiration date and can request amendments if necessary.

2.3.5 Appeals management

If the system issues a refusal of a data access application, the applicant has the right to appeal. The system may allow data applicants to provide their views through integrated communication means. If the issue remains unresolved, the system provides guidance for the user to formally request a comprehensive review of the case, seeking reconsideration of the initial decision.

3 REQUIREMENTS

3.1 Functional requirements

The functional requirements outlined in this paragraph have been formulated based on the ANALYSIS & DESIGN of HealthData@EU Infrastructure deliverables, incorporating insights into its current capabilities and limitations. Additionally, our internal views of the progress of TEHDAS2 Task 6.4 have informed the prioritization and feasibility of specific functional elements, ensuring alignment with project timelines and resource availability [10]. User interface, Identification, Authentication and Authorization (IAA) and communication requirements are presented separately.

3.1.1 User interface requirements

3.1.1.1 Allow users to select their preferred language

Requirement code:	DAAM_1.1
Requirement title:	The system should allow users to select their preferred language.
Actors involved:	- Data applicants, HDAB users, Trusted data holders.
Required features:	- Allow language selection of at least in one of the 24 official languages of the EU.
Detailed Description:	
Functionality	Description
Language selection	Data applicants can select their preferred language from the official EU languages supported by the CY-EHDS-2nd CP.
Full Translation	All textual content within the user interface, such as menus, buttons, labels, error messages, notifications, and tooltips, is fully translated and available in each language.
Prominent Language selection	The language selection feature is prominently accessible, allowing data applicants to switch between languages seamlessly and intuitively.

Automatic adjustment	The user interface automatically adjusts to reflect the selected language without any loss of functionality or data, ensuring a consistent and cohesive user experience across all language versions.
Remembering language preferences	The system remembers the user's language preferences for future connections (e.g., through cookies).

The required functionality will be inherited from the CY-EHDS-2nd CP.

3.1.1.2 Data access application and request templates

Requirement code:	DAAM_1.2
Requirement title:	The system must provide templates for data access applications and data requests applications.
Actors involved:	- Data applicants.
Required features:	- Provide standardised templates for data access applications and data requests.
Detailed Description:	
Functionality	Description
Data access application template	- Includes fields that data applicants need to complete, ensuring the inclusion of all necessary information as specified in the EHDS Regulation. - Guides data applicants through the application process, making it straightforward to provide all required details.
Data request template	- Contains fields specifically designed for data applicants to fill out, capturing the information mandated in the EHDS Regulation. - Guides data applicants through the request process, making it straightforward to provide all required details.
Logical flow and accessibility	- Forms follow a logical flow, guiding data applicants' step by step through the application process.

3.1.1.3 User friendly interface

Requirement code:	DAAM_1.3
Requirement title:	User friendly interface.
Actors involved:	- Data applicants.
Required features:	- Provide a user-friendly interface to complete the data access application or request form.
Detailed Description:	
Functionality	Description

The system provides an intuitive and user-friendly interface displaying the relevant application or request	- Forms are clearly structured with sections for required information, including user details, type of data requested, purpose of use, and compliance information. - The form prompts data applicants to fill out all necessary fields.

3.1.2 User Identification, authentication and authorization

Requirement code:	DAAM_2.1
Requirement title:	The system must allow for user IAA, including the option to enforce multifactor authentication.
Actors involved:	Data applicants, HDAB users, Trusted data holders.
Required features:	- Prompt to Log In (Incorporate some identification and authentication). - Establish authorisation (IAA) mechanisms.
Detailed Description: The system must implement Identification, Authentication and Trust Services (eIDAS)-compliant processes for data applicant IAA.	
Functionality	Description
IAA for data applicants	- Data applicants must identify themselves to access specific services, ensuring their actions can be tracked and audited. - Data applicants must be authenticated using their digital identity, with verification of identity accessible only to authorised data applicants.
IAA for HDAB users.	- HDAB users must identify themselves to access specific permissions, ensuring their actions can be tracked and audited. - HDAB users must be authenticated using their digital identity, with verification of identity accessible only to authorised users. - HDAB users must be authorised to review, manage, and provide decisions about access applications or requests, with assigned roles and levels of access.
IAA for Trusted Data holders.	- Trusted data holders must identify themselves to access specific permissions, ensuring their actions can be tracked and audited. - Trusted data holders must be authenticated using their digital identity, with verification of identity accessible only to authorised users. - Trusted data holders must be authorised to review and provide their comments about data access applications or requests, with assigned roles and levels of access.

The required functionality will be inherited from the CY-EHDS-2nd CP solution.

3.1.3 Applications management

The DAAMs must allow data applicants to select one or more datasets and complete a data access application or request form. This form may dynamically pre-fill form fields based on the dataset metadata, geographic origin, and applicant type. The system will provide secure functionality to save draft applications for later submission or modification. The system will also be able to receive data access applications or requests submitted at the HealthData@EU CP.

During the assessment process, the data applicant will be able to monitor the status of the application, withdraw the application, or provide further information if requested by the HDAB. At the end of the assessment process, the data applicant will be able to access the data permit with the decision of the HDAB.

3.1.3.1 Select datasets and application form

Requirement code:	DAAM_3.1
Requirement title:	The system must allow to select datasets descriptions and allow to select data access application or request forms.
Actors involved:	Data applicants.
Required features:	- Allow data applicants to select a dataset description. - Allow data applicants to select data access application or request form. - Adapt the content and structure of the data access application or request form based on the specific datasets being requested and the geographic origin of the data.
Detailed Description: The system should provide functionality to allow data applicants to select datasets from within the search datasets feature of the nHDsC component (CY-EHDS-2nd, D6.1).	
Functionality	Description

Allow data applicants to select a dataset description	- After searching, data applicants can select one or more datasets descriptions that meet their needs.
	- Applicants Authentication:
	  ○ The data applicants must log in using electronic means.
	  ○ Data applicants may need to provide evidence of affiliation to an entity (e.g., research centre, university, public sector bodies) to justify the purpose of access.
	- For dataset description selection the system may adopt a eCommerce Shopping Cart-similar Feature.

Allow data applicants to select data access application or request form	Data applicants can choose one of two options: - Create a Data Access Application - Create a Data Request Application
Adaptive Application or Request Form	- The form may automatically populates the origin of the dataset and includes specific fields to comply with legally binding national requirements related to the selected datasets.

	- The form may automatically populate information of the data applicants provided in the Log in feature.

3.1.3.2 Create / manage draft applications

Requirement code:	DAAM_3.2
Requirement title:	The system must enable data applicants to fill in and submit data access applications and requests.
Actors involved:	Data applicants.
Required features:	- Provide functionality that allows data applicants to save as draft, complete and submit data access application or requests efficiently. - Validate if all fields of data access application or request form were filled in and are compliant with the agreed format; - Show an error message in case any field is not compliant with the agreed standard and/or in case any mandatory field is missing; - Acknowledge a valid submission in case all fields are compliant with the agreed format and all mandatory fields have been correctly completed. - Securely store forms and allow the actions of editing or cancelling only to data applicant with permissions (IAA). - Provide data applicants with text editing functionalities on existing (but not submitted) forms.
Detailed Description: After selecting the dataset and the option of Data Access or Data Request Application, the system displays the form and allows for the completion and submission of the application. No modifications are allowed after the application submission.	
Functionality	Description
Applicant permissions and access	- Acknowledge the data applicant permissions (IAA) for creating, retrieving, deleting, and submitting data access applications or requests.
Access specifications	- Allow data applicants to read the data holder's access specifications per dataset, including for example Intellectual Property Rights. - Pre-populate the information of the data applicant.
Form fields	- Include mandatory fields (marked with an asterisk) and optional fields. - Provide fields with close-ended answers, multiple choice, single choice, numerical, or free text.
Automated data validation	- The system should provide automated or semi-automated checks for structured fields (e.g. phone numbers).
Progress indicator	- Show data applicants their progress in completing the form and remaining steps.
Auto-save functionality	- Ensure data applicants do not lose progress if they inadvertently close the form or face connectivity issues.

Tooltips and contextual help	- Provide tooltips or contextual help for each field, guiding data applicants on required information, especially for technical or legal terms.
Adapting to legal requirements	- Automatically adapt the form to legal requirements based on the selected datasets.
Ethical approvals	- Include details about necessary ethical committee approvals in the decision process.
File upload support	- Allow file uploads with checks on size and security including the purpose of the upload.
Review option	- Provide a review option before confirming submission.
Error notifications	- Alert data applicants with an error message and flag incomplete or incorrect fields prevent submission of incomplete forms.
Unique ID Generation	- Generate unique ID for tracking purpose upon submission.
Machine-readable output	- Ensure the output of a submitted application or request is in a machine-readable format.
Saving drafts	- Allow data applicants to save a draft of their form. - The system main implement autosaving of draft forms to ensure data applicants do not lose progress in case of system or browser crashes.
Accessing drafts	- Provide a dashboard with draft applications/requests where data applicants can access their drafts. - Prompt data applicants to log in with credentials to access the dashboard. - Display the draft applications/requests in the dashboard, allowing data applicants to open and continue working on them before submission.
Draft management	- Allow data applicants to cancel the draft form at any time before submission. - Allow data applicants to create a copy of draft.
Draft expiration	- The system may implement rules for draft expiration, defining a period of inactivity after which drafts will expire. - Notify data applicants of the expiration policy when saving their draft.
Estimate cost for data application creation	- The system should calculates an estimated cost for processing the data access or request application, based on the selected datasets and the information provided.

3.1.3.3 Manage submitted applications

Data applicants will be able to manage the applications they submit via a dedicated Dashboard. Depending on the status of the application, the system will provide different functionalities.

Requirement code:	DAAM_3.3
Requirement title:	The system must enable data applicants to manage their submitted applications.

Actors involved:	Data applicants.
Required features:	- View application and tracking status history. - Provide an option to update application with additional information, if requested by the HDAB. - Provide an option to withdraw their data access applications or requests from consideration at any stage (after submission) before obtaining a data permit/decision. - Be equipped with identification and authentication mechanisms to be able to withdraw an application or request (i.e. match the Login of the data applicant who submitted the application with the one that is trying to withdraw). - Access the HDAB decision / data permit.
Detailed Description: The system will allow data applicants to access and manage their submitted applications via a dedicated Dashboard.	
Functionality	Description
View/ access the applications submitted.	- Provide a dashboard with submitted data access or request applications where data applicants can access their submitted applications. - Allow the data applicants to view and track the complete status history of their applications via the dashboard.
Provide additional information	- Provide functionality for data applicants to update their application with additional information, if requested by the HDAB.
Withdraw application	- For applications or requests that are submitted the system displays a clearly labelled withdrawal option within the application and request dashboards. - Permissions verification: Before proceeding with the withdrawal, the system verifies that the data applicant has the necessary permissions. - Confirmation dialog: To prevent accidental withdrawals, the system presents a confirmation dialog explaining the consequences of withdrawal and requiring the applicant to confirm their intention to withdraw. - Status update: Upon confirmation, the application or request status updates to "Withdrawn" in the dashboard, and a confirmation message is displayed.
Access data permit	- For data access or request applications that the assessment process is completed the system allows data applicant to access the generated data permit/ decision.

3.1.4 Applications assessment

Upon submission, the HDAB authority responsible for evaluation performs the assessment of the data access or request application. The assessment process includes:

- Verifying the completeness of the application (pre-screening) and compliance with the data minimisation and protection principles.
- Allowing trusted data holders to provide technical or domain-specific assessments (where relevant - only for the data they hold).
- Requesting additional information from applicants when necessary.

After assessment the HDAB must be able to issue a decision to grant or deny access, with clear justifications communicated through the system. The assessment progress and decision must be tracked in the system and additionally, the NCPs must notify cross-border applicants of key updates, such as status changes or additional data requirements.

All HDAB users should be able to access the data access and request applications received. Authorized users (HDAB manager role) will be able to assign an application to a Reviewer (HDAB reviewer role) to perform the assessment of the application.

3.1.4.1 Access submitted applications

Requirement code:	DAAM_4.1
Requirement title:	The system must allow assessing data access applications and requests.
Actors involved:	- HDAB users (Application manager/ reviewer).
Required features:	- Receive data access applications or requests. - Apply IAA to perform tasks according to permissions. - Allow to view the content of the application or request.
Detailed Description: Upon receiving a data access application or request, HDAB users log into the system to assess the submitted applications.	
Functionality	Description
Data access and request dashboards.	- Provides a comprehensive overview of all received data access and request applications. - Enables efficient management and prioritisation of assessments.
User permissions.	- Prompts HDAB to authenticate their identities upon logging in. - Grants access only to users with necessary authorisations and permissions, ensuring that sensitive data is accessible only to authorised personnel. - Ensures that assessors have specific roles and responsibilities, allowing only authorised personnel to approve decisions, access, and process electronic health data according to their internal roles.
Display the submitted applications.	- If identification and authentication are successful, the system clearly displays submitted application and all included information. - The presentation is organised and user-friendly, allowing assessors to quickly review essential details for thorough evaluation. - Facilitates informed decision-making regarding data access approvals or rejections by having all relevant information readily accessible.

Receive data access or request applications submitted through the HealthData@EU CP.	- When a data applicant submits a data access or request application for the national dataset catalogue at the HealthData@EU CP, the system will receive the application via the NCP.

3.1.4.2 Publish information (Application public information) (to be implemented in the future under the scope of the 'Transparency Portal')

As soon as an application from a national data applicant is received, the system must make available to the public a summary of what has been requested (Public information of the project). The cross-border applications will not be included in this public view.

Requirement code:	DAAM_4.2
Requirement title:	The system must make available to the public the applications received via its user interface.
Actors involved:	- Public user.
Required features:	- Allow public users to view the applications submitted to the system.
Detailed Description:	
Functionality	Description
Display a public dashboard with the data access and request applications	- Provide a public dashboard with the data access or request applications submitted to the system via tis user interface. - For each application display the 'public information of the project' and their status. - As the assessment proceeds, the system will update the information and status of the applications in the public dashboard.

3.1.4.3 Flag for accelerate procedure

Requirement code:	DAAM_4.3
Requirement title:	The system must support accelerated applications or requests for public sector bodies and EU institutions.
Actors involved:	- HDAB users (Application manger)
Required features:	- Flag applications from public sector bodies and EU institutions which benefit from an accelerated procedure. - Display flag on applications from bodies and EU institutions in the dashboards from assessing bodies.
Detailed Description: Upon receipt of an application or request from public sector bodies and EU institutions, the system will be equipped with flagging and mechanisms to deal with accelerated procedures.	
Functionality	Description
Automatic Identification	- Identify the application as originating from a public sector body or EU institution with a legal mandate in public health.

Priority Flagging	- Flag the form with a e.g., "Accelerated procedure" label on the received applications dashboard for the HDAB users. - HDAB users should be able to view the purposes of the application and determine the degree of urgency.
Time-Tracking	- Display the deadline to allow complying with the timelines of the accelerated procedures.

3.1.4.4 Transfer application to trusted data holder for evaluation/assessment

Requirement code:	DAAM_4.4.1
Requirement title:	The system may allow to transfer data access and request application to trusted data holders for assessment.
Actors involved:	- HDAB users (Application reviewer), trusted data holders.
Required features:	- Have a functionality to provide temporary viewing and commenting permissions to trusted data holders. - Generate a link to the application in the system. - Share the application in the system with the trusted data holders.
Detailed Description: When reviewing a data access or request application, HDABs must have access to functionalities related to transferring the forms to Selected Trusted Data Holder in their systems.	
Functionality	Description
Sharing permissions	- Allow the addition of the name and contact details of trusted data holders. - Generate access to the form in the system for the trusted data holders.
Link sharing	- Share a notification with the trusted data holders contact details indicating that a data access or request application is pending their review.
Requirement code:	DAAM_4.4.2
Requirement title:	The system may allow trusted health data holders to evaluate data access application and requests.
Actors involved:	- HDAB users (Application reviewer), trusted data holders.
Required features:	- Allow trusted health data holders to review and comment the data access application or request, for the dataset they hold. - Send a message to the reviewer of the application that the evaluation of the trusted data holder is completed.
Detailed Description: After receiving a link to the application, trusted data holders must authenticate their identity in the system to gain access.	
Functionality	Description
Authentication	- Trusted data holders must authenticate their identity to gain access to the application or request (IAA).

Application display	- Once verified, the systems display the full application, including all submitted information, supporting documents, and any prior review comments.
Evaluation tools	- The system provides tools for evaluators to add comments, notes, and feedback directly within the system.
Review button	- Evaluators have the option to submit their review, which saves their assessment, including a proposal for a decision.
Alert trigger	- This action triggers the relay of a message to the HDAB that the review is completed, and the review and assessment cycle can continue.

3.1.4.5 Update status and timelines

Requirement code:	DAAM_4.5
Requirement title:	The system must provide automated updates on data access and request applications status and timelines.
Actors involved:	- HDAB users (Application manager, reviewer).
Required features:	- Display the status of the received data access and request applications in a dashboard. - Display a time-tracking functionality with a text indicating the working days to provide a decision. - Trigger a system status change when steps within a workflow (i.e. review and assessment cycle) are completed. - Should allow authorized users the manually change the status/timelines. - Exchange information with NCP to keep the status of the cross-border applications aligned and updated between all systems.
Detailed Description: After receiving a data access or request application, data applicants follow up on the workflow/progress of the assessment.	
Functionality	Description
Workflow status tracking	- The workflow steps are paired with statuses that change as the assessment process progresses. - The statuses are visible from the applications dashboards of the assessing bodies and include information on the status of the applications.
Status* categories for Assessing Bodies	- “Received”: When all relevant assessing bodies have received the data access application or request. - “Under review”: When assessing bodies have started their review and assessment (including under review by Trusted Data Holder). - “Extended review”: When assessing bodies may need more time to assess the application or request in accordance with the reasons established in the EHDS Regulation. - “Awaiting additional information”: When data applicants are requested to provide more information.

	- "Granted": When the assessing bodies decide to grant the data request or permit. - "Refused": When the assessing bodies decide to refuse the data request or permit. - "Withdraw": When the data applicant decides to withdraw the application or request.
Time-tracking functionality	Displays the number of days since submission and the deadline to move to the next step of the workflow according to the EHDS Regulation timeframes.
Automatic status updates	The status of the data access or request application automatically changes during the different stages of the workflow.
Status* categories for Data applicants	- "Submitted": When the application is successfully submitted but not yet distributed. - "Delivered": When all relevant bodies have acknowledged receipt. - "Under review": When assessing bodies have started their review and assessment (including under review by Trusted Data Holder). - "Extended review": When assessing bodies may need more time to assess the application or request in accordance with the reasons established in the EHDS Regulation. - "Awaiting additional information": When more information is requested. - "Granted": When the request or permit is granted. - "Refused": When the request or permit is refused. - "Withdrawn": When the applicant withdraws the application or request.
Status updates coordination	The system notifies the HealthData@EU CP via NCP for status changes of cross-border applications received.

* The status categories for Data applicants and Assessing Bodies will be aligned with TEHDAS2 D6.4 [10].

3.1.4.6 Extend the assessment process

Requirement code:	DAAM_4.6
Requirement title:	The system must allow for extending the assessment process.
Actors involved:	- HDAB users (Application manager).
Required features:	- Allow to extend the period of responding to a data access or request application. - Allow to include a free text justification of why extension is needed. - The system must change the status of the application in the dashboard to "*Extended review*". - Push notifications to NCP for cross-border applications to update the status to "Extended review". - Trigger a communication to the data applicant about the change of the status and the reasons of the extension.
Detailed Description:	

During the assessment of a data access or request application, authorized users can extend the period of assessment up to 3 months. The assessor must inform the data applicant of such extension and the reasons for it.	
Functionality	Description
Extension of response period	- A feature labelled “Extend decision” is provided in the assessment interface. ○ If selected, prompt to provide a justification for extension, must be provided as free-text entries. - Once confirmed, the DAAM system should update the application status to “Extended review”.
Notification and communication	- The system informs data applicants about the status change and provides reasons for the extension. - Data applicants can view the "*Extended review*" status on the applicable dashboards, subject to identification and authentication, to ensure the applicant's identity matches the original submission. - The system pushes notifications to - For cross-border applications, the system notifies the NCP to push notifications to the HealthData@EU CP updating the status to "*Extended review*."

3.1.4.7 Request additional information

Requirement code:	DAAM_4.7
Requirement title:	The system should allow for requesting additional information during the assessment process.
Actors involved:	- HDAB users (Application manager, reviewer), Data applicants.
Required features:	- Allow to request additional information from the data applicant. - Allow to include a free text justification of why/what additional data is needed and how it should be provided.
Detailed Description:	
Functionality	Description
Option to request additional information	- Display the option to request additional information when assessing the form. - The system prompts the assessor to provide a detailed explanation regarding the additional data needed, why it is required, and how it should be provided.
Status update for additional data requests	- Automatically update the status of the application to "awaiting additional information". - Stop the clock of deadline for review. The clock restarts when it is put back to "under review" status (i.e. when the additional information is submitted.

Automated message	- The system automatically sends the assessor's message to the data applicant with a link to the data access application or request. - For cross-border application, the assessor's message is sent to the NCP that is responsible to forward the message in the appropriate format to the HealthData@EU CP. - The system supports free-text messages and file uploads. Each message displays the sender's identity, a timestamp, and a response timeline, aligned with standard procedures.

3.1.4.8 Receive application updates

Requirement code:	DAAM_4.8
Requirement title:	The system must allow for receiving application updates during the assessment process.
Actors involved:	- HDAB users (Application reviewer), Data applicants.
Required features:	- Allow to receive additional information from the data applicant. - Allow to receive withdrawal of applications from the data applicant.
Detailed Description:	
Functionality	Description
Receive additional information	- Receive additional information from a national data applicant or the NCP (for a cross-border application).
Receive withdrawal of application	- Receive an application withdrawal request from a national data applicant or the NCP (for a cross-border application).
Status update when receiving additional information	- Automatically update the status of the application to "under review". - Restart the clock of deadline for review.
Status update when receiving a withdrawal request.	- Automatically update the status of the application to " Withdrawn".

3.1.4.9 Approve / reject

Requirement code:	DAAM_4.9
Requirement title:	The system must allow for rejecting or approving data access and request Applications.
Actors involved:	- HDAB users (Application manager, reviewer).
Required features:	- The system must allow to provide a decision after the assessment of a data access or request application. - Push notifications to the NCP for cross-border status application updates (update status to "grated" or "refused").
Detailed Description:	

Functionality	Description
Actions	- "Grant": Grants full approval of the application or request. - "Grant under conditions": Grants partial approval of the application or request (e.g., only for dataset A and B, for purpose 1 but not 2, etc.). If "Grant under conditions" is selected, the system prompts the user to provide a justification for the conditions in a free-text field before submission. - "Refuse": Denies the application or request. If "Refuse" is selected, the system prompts the user to provide a justification for the rejection in a free-text field before submission.
Status update for HDABs	- The system automatically updates the status to "granted" or "refused" in the dashboard. The NCPs push this status change to the HealthData@EU CP.

3.1.4.10 Communicate outcome

Requirement code:	DAAM_4.10
Requirement title:	The system must communicate the outcome of the assessment.
Actors involved:	- HDAB users (Application manager, reviewer), Data applicants.
Required features:	- Send a message to the data applicant about the outcome of the assessment of the data access or request application.
Detailed Description: Once the assessment of a data access or request application is completed, the system must notify the applicant of the assessment decision. National data applicants will be notified via an integrated communication feature. Cross-border application notifications will be pushed to the NCP. The communication includes details of the outcome and any relevant instructions or next steps, as well as information on how to appeal the decision.	
Functionality	Description
Notification of assessment decision	- Notify the applicant of the assessment decision through an integrated communication feature. - Include details of the outcome (decision) and any other relevant instructions or next steps.

3.1.4.11 Other

Requirement code:	DAAM_4.11.1
Requirement title:	Track assessment progress and automatically notify stakeholders of key actions.
Actors involved:	- Data applicants.
Required features:	- Inform key stakeholders when the status of an application or request has been updated.
Detailed Description:	

Functionality	Description
Automatic status changes	Trigger status changes in the dashboards as the review and assessment process progresses.
Timestamp recording and communication	- Record each status change with a timestamp. - Communicate status changes for cross-board applications to the NCP.
Automated communication to data applicants	- Facilitate automated messages to data applicants, informing them of status changes. - Identify the contact details of the data applicant and relay a message indicating the status change.
Requirement code:	DAAM_4.11.2
Requirement title:	The system must maintain a detailed audit trail of all assessment actions and decisions.
Actors involved:	- HDAB users.
Required features:	- Record relevant data about the receival, assessment and decision of a data access request or application. - Record the messages exchanged during the process.
Detailed Description: The system must implement a robust logging mechanism to maintain detailed, identifiable logs of all assessment activities triggered within the system. These logs include precise timestamps and capture the following key information:	
Functionality	Description
Loggin mechanism	- Record data access application receival date and time. - Record data requests receival date and time. - Record the assessor user reviewing the application or request. - Record and process the login of the data applicant. - Record changes in the status of each application and request. - Record message exchanges through the integrated communication channel. - Record decisions on those applications or requests. - Record the date of decision.
Audit accessibility	- Ensure this information is findable by appropriate authorities for audit purposes.

3.1.5 Fees management

Calculates and communicates transparent, non-discriminatory, and proportionate fees to make electronic health data available to data users. These fees will be communicated transparently before the submission of the data access application or request. Generates invoices to be paid when the data permit is generated.

3.1.5.1 Advertise the fee structure and calculation methods, making them publicly available (to be implemented in the future under the scope of the 'Transparency Portal')

Requirement code:	DAAM_5.1

Requirement title:	The system should advertise the fee structure and calculation methods, making them publicly available.
Actors involved:	- HDAB users, Public user.
Required features:	- Provide a dedicated space for displaying fee structure - Provide a publicly accessible space without login/registration
Detailed Description: The CY-EHDS-2nd CP will feature in the future a dedicated space under the scope of the 'Transparency Portal' where the entire fee structure for accessing electronic health data is clearly outlined. Any user can view the fee structure without requiring login or registration	
Functionality	Description
Publicly available of fee structure	- Provide details on the tiered fee system
Fee categories	- Standard Fees. - Reduced Fees. - Public Sector Data Holders
Detailed fee description	- Break down fees into specific components explaining cost calculations, including: ○ Administrative fees (processing, application management). ○ Data preparation fees (anonymisation, pseudonymisation). ○ Additional service fees for complex or customised data requests.

3.1.5.2 Provide functionalities to estimate costs incurred for accessing electronic health data

Requirement code:	DAAM_5.2
Requirement title:	The system may provide functionalities to estimate costs incurred
Actors involved:	- HDAB, Data applicants, Data holders.
Required features:	- Provide a cost simulator functionality that allow applicants to estimate costs incurred for accessing electronic health data.
Detailed Description: The system features a dedicated space where data applicants can find a fee calculator/simulator tool to simulate the cost of accessing health data.	
Functionality	Description
Fee calculator/ fee simulator tool	- Provides an instant, real-time estimate of costs. - Takes into account different fee categories (tiers) and complexities. - Dynamically adapts according to the input and parameters of the access (e.g., data type, scope of the request).

3.1.5.3 Dynamically inform applicants about expected fees as they prepare and submit their requests

Requirement code:	DAAM_5.3

Requirement title:	The system should dynamically inform applicants about expected fees as they prepare and submit their requests.
Actors involved:	- Data applicants.
Required features:	- Provide cost calculation functionalities that allow applicants to know the expected fees as they prepare and submit their applications and requests.
Detailed Description: The system is equipped with a real-time cost calculation functionality in the interface were data applicants' complete data access and request applications.	
Functionality	Description
Real-Time Cost Calculation	- Calculate and validate fees proportional to the actual costs incurred, reflecting the specific services requested by the participant.
Fee Summary Prompt:	- When applicants select to submit a data access application or request, a prompt appears summarising the expected fees based on their selected data and service.

3.1.5.4 Keep a log of the incurred costs throughout the assessment process & notify the applicant in the case of withdrawal

Requirement code:	DAAM_5.4
Requirement title:	The system shall keep track of the incurred costs during the assessment process and notify the costs to the applicant in case of withdrawal.
Actors involved:	- HDAB users (Application reviewer), Data applicants, Data holders.
Required features:	- Keep a detailed record of costs incurred during the processing of applications, including administrative review, data preparation, and other related expenses. - Notify the applicant about the incurred fees (and their breakdown).
Detailed Description: The system maintains a record of costs incurred during the processing of applications, including administrative review and data preparation. In the event of withdrawal, these systems calculate the exact costs incurred up to that point and generate an invoice.	
Functionality	Description
Cost recording	Maintain a record of costs incurred during the processing of applications, including administrative review and data preparation.
Cost calculation and invoicing:	- Calculate exact costs incurred (up-to date). - Generate an invoice for the incurred costs.
Automated notification	- If an applicant decides to withdraw, the system automatically notifies the applicant. ○ The notification includes a summary of the incurred costs up to that point and provides the invoice with relevant payment.

	○ For cross-border application, if the system receives a withdrawal application update, it automatically relays to the NCP the notification to the applicant.

3.1.5.5 Generate invoices with fee breakdowns

Requirement code:	DAAM_5.5
Requirement title:	The system may enable generating invoices with fee breakdowns
Actors involved:	- HDAB users (Application manager), Data applicants, Data holders.
Required features:	- Provide a functionality to generate standard invoices and invoices generated when an applicant withdraws their request.
Detailed Description: The system provides functionality to generate invoices that include a detailed breakdown of fees for data access & request application review and data provision in the SPEs.	
Functionality	Description
Invoice generation	Generate invoices with a detailed breakdown of fees for data access application review and data provision
Automatic data permit and invoice generation	For applications from a national data applicants, once the HDAB approves the data access or request application, the system automatically generates an invoice detailing the fees incurred and payment details.
Invoice generation on withdrawal	- Automatically generate an invoice with a detailed breakdown of fees incurred up to the point of withdrawal when an applicant withdraws their application. This ensures the applicant is only charged for services provided up to that moment.

3.1.5.6 Allow data applicant to request a negotiation of fees

Requirement code:	DAAM_5.6
Requirement title:	The system may allow for disagreements on fees and provide resolution mechanisms
Actors involved:	- HDAB users (Application manager, reviewer), Data applicants, Data holders.
Required features:	- Allow to comment on the fees requested.
Detailed Description: Data applicants may request a negotiation of the fees. They can provide their comments through the integrated communication means of the systems linked to the application or request.	
Functionality	Description
Dispute communication	- Data applicants comment on fee disagreements in the integrated communication means of the system. - HDABs can respond in the same integrated communication means of the systems.

Resolution Mechanism	- If negotiation does not lead to an agreement, the system facilitates the process by providing a step-by-step guide. o The guide explains how to submit a resolution mechanism request where resolution mechanisms can be discussed.

3.1.5.7 Allow applicants to pay the invoice within the application

Requirement code:	DAAM_5.7
Requirement title:	The system should allow applicants to pay the invoice within the application.
Actors involved:	- HDAB users (Application manager, reviewer), Data applicants, Data holders.
Required features:	- Enable secure payments for both standard invoices (with data permits) and invoices generated when an applicant withdraws their request. - Support multiple payment methods to accommodate various applicant preferences.
Detailed Description: Once the fees are agreed upon, the system allows applicants to pay invoices directly within the portals/systems.	
Functionality	Description
Payment integration	- For system provides a secure link to a dedicated payment platform through integrated communication means.
Payment interface	- Applicants are redirected to a payment interface that is integrated with the HDAB Portal. - The interface supports multiple payment methods, e.g., credit cards, bank transfers, accommodating different applicant preferences.
Security and compliance	- Robust encryption and compliance with industry standards ensure that all financial transactions are protected, maintaining applicant trust and safeguarding sensitive data.
Payment confirmation	- Once the payment is processed, applicants receive immediate confirmation of their transaction.

3.1.5.8 Allow for redistribution of (part of the) fees towards data holders as compensation

Requirement code:	DAAM_5.8
Requirement title:	The system should allow for redistribution of (part of the) fees towards data holders as compensation.
Actors involved:	- HDAB uses (Application manager, reviewer), Data holders.
Required features:	- Allow a generation of notice for data holders to receive compensation. - Send automated notifications to data holders about pending and completed compensation transactions.
Detailed Description:	

The system establishes an efficient and transparent system for compensating data holders based on their data contributions. This process involves the following functionalities:	
Functionality	Description
Notification and Information	- Generate a notice for each data holder detailing their upcoming compensation. - inform the data holders. - Generate automatic notice when the reimbursement has been sent.

3.1.5.9 Maintain a comprehensive log of all fee-related transactions

Requirement code:	DAAM_5.9
Requirement title:	The system must maintain a comprehensive log of all fee-related transactions.
Actors involved:	- HDAB users, Data holders, Data applicants.
Required features:	- Track all fee-related activities, including invoicing, payments, fee adjustments, and disputes, ensuring every transaction is recorded in detail. - Include specific data points such as transaction dates, amounts, fee breakdowns, and payment statuses to provide a full audit trail. - Ensure that the log is securely stored and easily accessible for auditing purposes, both for internal use and external regulatory review.
Detailed Description: The system maintains a comprehensive log of all fee-related transactions to ensure transparency, traceability, and regulatory compliance.	
Functionality	Description
Fees Log Information	- Transaction ID: A unique identifier for each transaction to facilitate easy tracking and reference. - Date and Time of Transaction: The exact date and time when the transaction was initiated and completed. - Applicant Details: Information about the applicant who made the payment, including applicant ID, name, and contact information. - Invoice Number: The corresponding invoice number associated with the transaction for cross-referencing. - Amount Paid: The total amount paid in the transaction, including a breakdown of any taxes, fees, or additional charges. - Payment Method: The method used for the payment (e.g., credit card). - Status of Payment: The current status of the payment (e.g., pending, completed, failed). - Purpose of Payment: A description of what the payment was for (e.g., standard application fee, withdrawal fee). - Transaction Outcome: Details on whether the transaction was successful, failed, or pending, including any error codes or messages in case of failure.

	- Confirmation or Receipt Number: The confirmation number or receipt number provided to the applicant once the payment was successfully processed, including payments from data applicants to HDAB, as well as payments from HDAB to data holders. - Administrative Notes: Any additional notes or comments from the administrative staff regarding the redistributions of fees with data holders, if applicable.
Retention of Logs	- Retain these logs for the required regulatory period, allowing for future reference and compliance checks.

3.1.5.10 Provide automated reminders for upcoming payments and due dates to prevent late fees and non-compliance

Requirement code:	DAAM_5.10
Requirement title:	The system may provide automated reminders for upcoming payments and due dates to prevent late fees and noncompliance.
Actors involved:	- Data applicants.
Required features:	- Track the status of the payment requests throughout its lifecycle. - Provide alerts to data applicants of approaching deadlines.
Detailed Description: The system includes a time-tracking functionality to monitor payment request deadline dates as per the regulation.	
Functionality	Description
Time-Tracking Functionality	- Monitor payment request deadline dates. - When a deadline approaches its expiration, the system trigger alerts to notify relevant stakeholders.
Notification System	- Notifications are sent to the data applicant

3.1.6 Data permits management

Once a data access application is approved, the system prepares and issues the data permit, including any necessary annexes that outline the terms and conditions for data access and use (including the SPE where the data processing will occur).

The NCPs share the data permit with the Data User through integrated communication means. The system tracks the permit's status throughout its lifecycle, providing updates on approvals, amendments, and impending expirations. Users receive automatic notifications when a permit is approaching its expiration date and can request amendments if necessary.

3.1.6.1 Issue data permit

Requirement code:	DAAM_6.1
Requirement title:	The System must allow for preparation (generation and issuance) of a data permit with annexes.

Actors involved:	- HDAB users, Data applicants.
Required features:	- Automatically generate a machine-readable data permit triggered by the approval of the data access application (i.e. when the status of the system changes to "granted"). - Automatically generate a human-readable data permit (based on the template) triggered by the approval of the data access application (i.e. when the status of the system changes to "granted"). ○ Automatically pre-fill certain information in the draft data permit stemming from the data access application - The system must make the human-readable data permit available to the data applicant via the dedicated Dashboard. - For cross-border applications the system must push notifications to the NCP and draft data-permit.
Detailed Description:	
Functionality	Description

Automatic human-readable data permit generation	- Generate human-readable data permits incorporating prefilled information based the requirements of the EHDS Regulation.
	- Ensure essential information is consistently captured and presented, including:
	  ○ Purpose and scope of use.
	  ○ Data minimisation, security, and anonymisation measures.
	  ○ Time limits, geographical restrictions, and other regulatory requirements.

Automatic machine-readable data permit generation	- The system may generate machine-readable data permits to be used as a digital token to configure the SPEs according to the permit.
Share functionality	- Provide a confirmation functionality to finish the draft data permit generation. - Prompt HDAB users to review the contents of the draft data permit, confirming that all details are accurate and complete before submission.
Efficient communication	- Push the human-readable data permit directly to the data applicant via the integrated communication means of the systems. - Push the machine-readable data permit directly to the SPE operators to request the creation of the SPE for data analysis. - For cross-border applications, push data permits and notifications to the NCP.

3.1.6.2 Enable exchanges about data permits conditions

Requirement code:	DAAM_6.2
Requirement title:	The System must enable exchanges about data permits conditions.
Actors involved:	- HDAB users, Data applicants.

Required features:	- Provide the option for the data applicant to preview the data permit.
Detailed Description: Following the communication of the assessment outcome, the system prepares a data permit.	
Functionality	Description
Sending the Data Permit	- The system sends the data permit through the integrated communication means of the system to the data applicant for review.
Applicant Review Options	- The data applicant logs into the system (IAA). - The data applicant reviews the data permit and decides to: ○ Comment/ask about the conditions of the data permit.
Notification and Review	- The HDAB user receives notification through the integrated communication means and review the exchange.
Adjustment and Resending	- If the HDAB agrees, they make the necessary adjustments to the data permit. - The system re-sends the adjusted data permit through the integrated communication means.

3.1.6.3 Store and share data permit and all its relevant information

Requirement code:	DAAM_6.3.1
Requirement title:	The System must allow for the storing and sharing of a data permit and all its relevant information.
Actors involved:	- HDAB users, Data applicants.
Required features:	- Update the status of the data permit to “grated/active”. - Securely store issued data permits. - Share the data permit with data users. - Push notifications to the NCP to centralise data permits.
Detailed Description:	
Functionality	Description
Retention of Data Permits:	- The system retains copies of the data permits (both human-readable and machine-readable).
Secure storage	- The system securely stores the data permit, ensuring it is readily accessible for future reference while maintaining confidentiality and integrity.
Secure sharing	- The system securely shares the data permit with the relevant data users.
Status update	- The system updates the dashboards of data permits and promptly updates the status of the data permit to “granted/active”. - The system notifies the NCP for cross-border applications updates to align HealthData@EU CP dashboards of data permits and promptly update the status of the data permit to “granted/active”.

Requirement code:	DAAM_6.3.2
Requirement title:	The System must track the status of the data permit throughout its lifecycle.
Actors involved:	- HDAB users, Data applicants.
Required features:	- Track the status of the data permit throughout its lifecycle. - Share any updates in cross-border data-permits with the HealthData@EU CP via the NCP.
Detailed Description:	
Functionality	Description
Real-time status updates	- Update the Data Permits Dashboard to reflect changes in real-time as the data permit progresses through its lifecycle stages.
Lifecycle stages	- Include statuses such as "Open", "Granted/Active", "Amended", "Renewed", "Revoked", "Expired". - Change the status to "Amended" if any amendments are made, ensuring transparency over the permit's history.
Information sharing	- Share the updated status in the systems dashboard through the NCP with the HealthData@EU CP.

3.1.6.4 Enable users to request amendments to data permits

Requirement code:	DAAM_6.3.4
Requirement title:	The System should enable users to request amendments to data permits.
Actors involved:	- HDAB users (Data permit manager), Data applicants.
Required features:	- Allow for the data users to request changes to active data permits through the integrated communication feature of the system.
Detailed Description: When a health data user needs to update a data permit, they submit a request for an amendment. The system may facilitate this process by guiding the data user to use the integrated communication means of the system and send comments or suggestions.	
Functionality	Description
Amendment request	Allow the data user to submit a request for an amendment by sending comments or suggestions in integrated communication means of the system.
Review of request	The HDAB reviews the request to amend the data permit.
Adjustments and resending	- If the HDAB agree, the system must allow to make the necessary adjustments to the data permit. - The system re-sends the amended permit for review.
Disagreement process	- If the HDAB do not agree with the amendment request, they communicate this to the data user. - The system communicates the decisions to the data user with guidance for next steps.

3.1.6.5 Maintain logs of data permit actions

Requirement code:	DAAM_6.3.5
Requirement title:	The system must maintain logs for data permit actions.
Actors involved:	- HDAB users.
Required features:	- Track all permits under their jurisdiction.-related activities ensuring every activity is recorded in detail. - Include specific data points such as dates, actions, etc. to provide a full audit trail. - Ensure that the log is securely stored and easily accessible for auditing purposes, both for internal use and external regulatory review.
Detailed Description: The system maintains a comprehensive log of all data permit-related activities to ensure transparency, traceability, and regulatory compliance.	
Functionality	Description
Data Permit Log Information	- Permit ID: A unique - HDAB responsible - Date and Time of issuance - Applicant Details - Purpose and scope of use. - Data minimisation, security, and anonymisation measures. - Expiration date - Geographical restrictions - Other regulatory requirements.
Retention of Logs	Retain these logs for the required regulatory period, allowing for future reference and compliance checks

3.1.7 Appeals management

If the system issues a refusal of a data access application, the applicant has the right to appeal, by providing their views through integrated communication means. If the issue remains unresolved, the system provides guidance for the user to formally request a comprehensive review of the case, seeking reconsideration of the initial decision.

3.1.7.1 Allow communication for appeals on data permit refusals.

Requirement code:	DAAM_7.1
Requirement title:	The System should allow communication for appeals on data permit refusals.
Actors involved:	- Data applicants.
Required features:	- The system should provide instructions to the data applicant to submit an appeal.
Detailed Description:	

Once the refusal of a data access request is communicated to the applicant, the data applicant may intend to submit an appeal.	
Functionality	Description
Facilitation of Appeal Process	- The system includes in the communication of the decision a step-by-step guide on how to submit a request for a resolution mechanism (i.e. via email).

3.1.7.2 Change decisions after the appeal process.

Requirement code:	DAAM_7.2
Requirement title:	The System must allow for changing decisions after the appeal process.
Actors involved:	- Data applicants.
Required features:	- Allow to modify the decision of a data access application or request - Allow to provide a justification for decision - Allow to upload supporting documentation for the decision
Detailed Description: If the resolution mechanisms determine that the data access application can be approved after the appeal, the system must have the functionality to find the data access application, open it, and modify the outcome.	
Functionality	Description
Modify decisions functionality	- Allow finding and opening the data access application. - Allow to modify the outcome through a "Modify the decision" functionality triggering directly display of the two decision actions possible.
Decision actions	- Provide two distinct actions in the data access application or request review interface: ○ "Grant": For granting full approval of the application and generating a data permit. ○ "Refuse": For rejecting the application.
Update	- Update the application or request status in the appropriate dashboards after the decision action.
Notification	- For cross-border applications the system pushes a notification about the status update to the NCP. - Send a message through the integrated communication means of the system with the updated decision to the data applicant.

4 SPECIFICATIONS

4.1 DAAMs processes

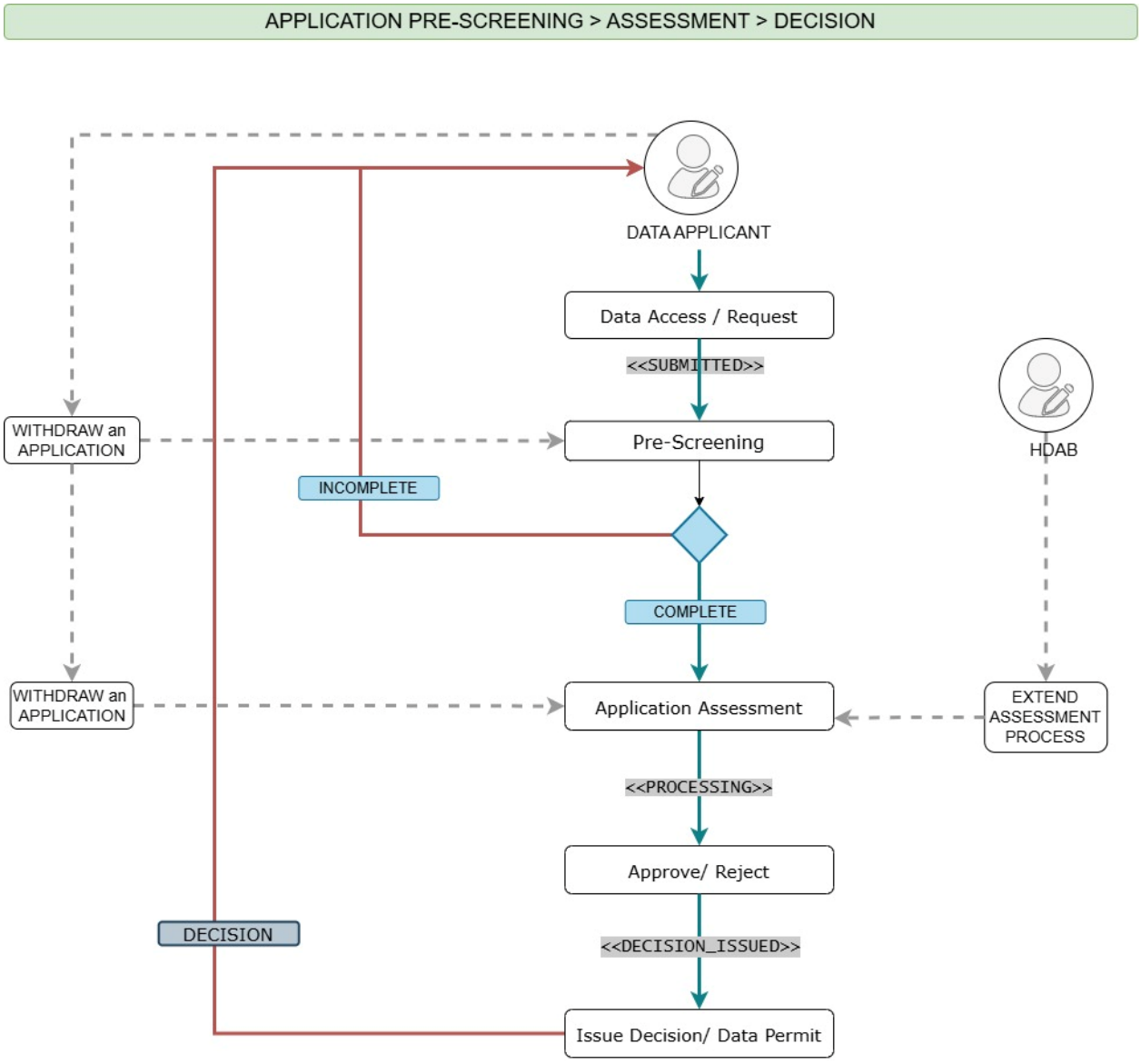

Figure 5: Application lifecycle (submission to Decision).

4.1.1 Application assessment to Decision

Figure 5 shows the basic process flow from application submission to the HDAB's decision. A data applicant fills in a data access or request application and submits it to the HDAB for assessment. HDAB may also receive a cross-border application from the HealthData@EU CP via the NCP (not shown here).

The application assessment starts from the Pre-screening step (completeness check) to verify that required fields are filled with plausible content [9]. If the application is assessed as "INCOMPLETE" the data applicant is informed of the missing or invalid fields to provide additional information. If the application is assessed as "COMPLETE" the flow proceeds to the assessment step. HDAB process/ evaluates the application to decide if the data access or request can be granted or not. The decision (positive or negative) is documented (i.e. using the Data Permit template [9]) and the outcome is communicated to the data applicant. Other processes

are then involved like the 'Data permits management' and the 'Fees management'. Upon issuing a decision, the system activates other processes such as the 'data permits management' and the 'fees management'. DAAM's technical specifications will be finalized based on the TEHDAS2 T6.4 outcomes [10] and included in upcoming deliverables of the CY-EHDS-2nd project.

4.1.2 Cross-border data access or request applications

The message sequence diagram in Figure 6 shows the processing flow of incoming cross-border applications, as discussed in TEHDAS2 Task 6.4 "Technical specifications for Health Data Access Bodies" [10]. Based on these discussions, the interaction involves three components: the HealthData@EU CP, the NCP (CY-EHDS-2nd WP8) and the DAAMs.

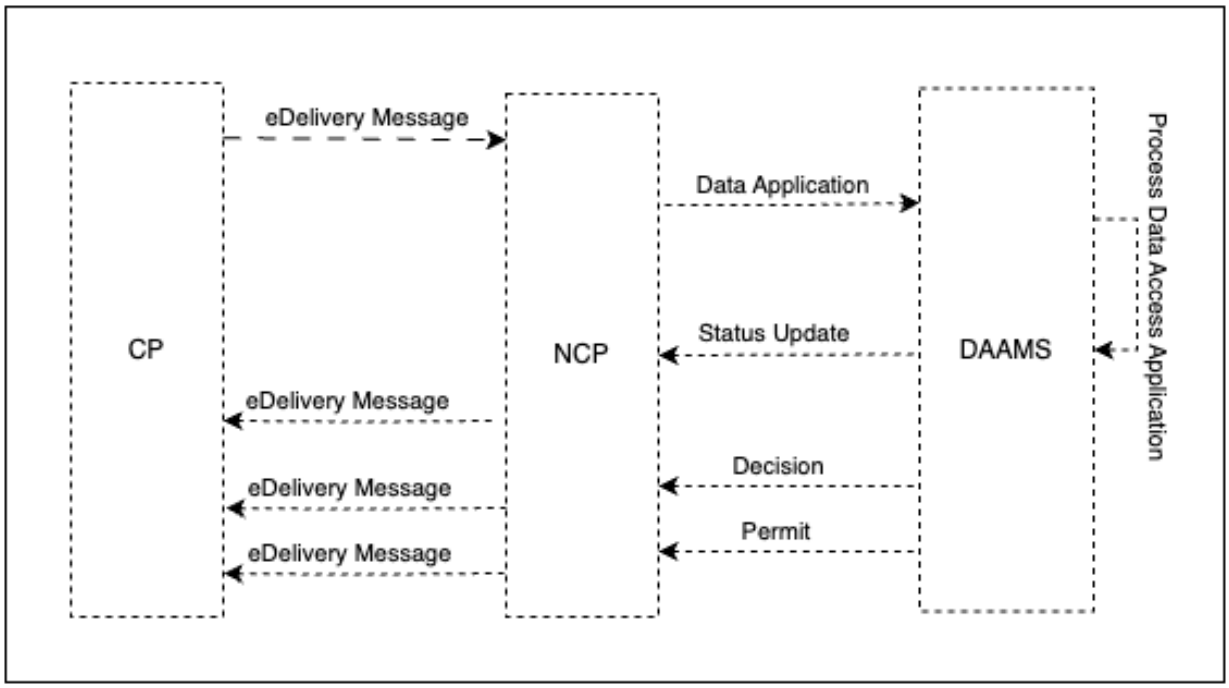

Figure 6: Message sequence diagram showing the communication between DAAMs, NCP, HealthData@EU CP [10]

All cross-border communication must flow through the NCP, which acts as the sole interface between the CY-EHDS-2nd infrastructure and the HealthData@EU CP [10]. The requirements specification of this communication is defined in CY-EHDS-2nd D8.1 "National Connector for Cross-border gateway Requirements and Specifications".

The sequence proceeds as follows:

1. Reception by NCP: The HealtData@EU CP forwards a cross-border application to the NCP of the national dataset catalogue (WP6, nHDsC).
2. Forwarding to DAAMS: The NCP validates the incoming payload and forwards it to DAAMS. The payload includes structured metadata such as applicant identity, legal basis, purpose of use, dataset references, and supporting documentation.
3. Local processing: DAAMS processes the request according to national regulations and internal procedures, in compliance with Articles 51 and 53 of the EHDS Regulation.

4. Status updates: Throughout the lifecycle of the application, DAAMS sends status updates (e.g., received, under review, pending clarification, decision made) to the NCP. The NCP relays these updates to the HealthData@EU CP to keep the applicant informed.

5. Application decision and response: DAAMS sends the application decision—approval or rejection—back to the NCP, including any accompanying metadata such as justification, conditions, or validity period.

6. Permit transmission: If access is granted, HDAB generates a data permit in the EU-standard format and forwards it to the NCP. The NCP then forwards the permit to the HealthData@EU CP, which delivers it to the requester.

This communication model ensures that all message exchanges remain traceable, secure, and fully aligned with the interoperability requirements defined in the EHDS Regulation. The technical specifications of the messages and structures to be exchanged will be defined in TEHDAS2 D6.4 [10] and will be incorporated into upcoming deliverables of the CY-EHDS-2nd project.

4.2 DAAMs module of CY-EHDS-2nd CP

The DAAM system is one of the core functional modules of the CY-EHDS-2nd CP, and its design will adhere to microservices architecture principles. Accordingly, this chapter outlines our considerations to decomposing the system's functionalities into discrete services, considering recommendations from the "ANALYSIS & DESIGN of HealthData@EU Infrastructure" deliverables [5]. Detailed technical specifications and final implementation details will be provided in the upcoming deliverable D5.2 "DAAMs Implementation and Piloting".

DAAMs will inherit/use core functions of the CY-EHDS-2nd CP infrastructure such as the national identity gateway (CY Login), for IAA mechanisms, and the logging, monitoring, and audit trail capabilities.

4.2.1 Applications management and assessment

This section shows a breakdown of the data access and request applications management module, outlining the services and systems involved in their creation and assessment Table 22. The domain encompasses the complete lifecycle of data access and request applications, from initial submission through assessment to final decision-making and notification.

Table 22: Applications management and assessment Core Features

Feature/ service	Description
User IAA	Confirms user´s identity and ensures that the user has the right permissions to access and interact with the system. ○ Verifies user identity and permissions before allowing access to the portal and data access features. ○ Ensures secure user identification and authorisation to initiate and submit data access/request applications. ○ Ensures secure user authentication to interact with the portal and initiate data access/data request application. ○ Authenticates users for assessing data applications.
Applicationsh management	Manages the entire process of creating, submitting and revision of applications.

	○ Manages the creation and submission of applications, ensuring users can initiate, modify and submit application forms. ○ Coordinates the assessment process of submitted applications, including routing the assessment to relevant bodies.
Applications status monitoring	Tracks the progress of applications and provides users with updates on their status. ○ Tracks the progress of applications from submission to decision making, providing to the users, status updates in the portal.
Decisions coordination and communication	Ensures that decisions are communicated to users and relevant stakeholders. ○ Facilitates communication of assessment outcomes to data applicants, ensuring users are informed about the final decision.
Assessment of data access applications and compliance	Reviews applications, ensuring the compliance with legal and data protection requirements. ○ Evaluates applications and assesses compliance with regulation, before providing access to the requested data. In case Trusted Data Holders are selected for assessing the applications, they will play a key role in approving or rejecting applications.

The term 'applications' refers to both data access or data request applications.

Proposed services:

Following the CY-EHDS-2nd CP design principles we can consider the following microservices to support the domains' core features as outlined in **Error! Reference source not found.**:

- *Data application*: to provide functionalities for revision, creation, submission and tracking of data access and request applications.
- *Cost estimation microservice*: to provide a cost estimation calculation for the type of application based on the input data and selected datasets before application submission.
- *Application status microservice*: to provide a real-time tracking of the application status updates for the data users.

Integrations:

The module integrates with the Dataset Catalogue component for dataset selection.

4.2.2 Fees management

This section outlines specifications for calculating, communicating, invoicing, and managing fees associated with data access and request applications. This includes providing an estimated fee during the application process for review prior to submission, as well as issuing a final invoice upon approval of the data application.

Table 3 3: Fees Management Core Features

Feature/ service	Description
User IAA	Validates user identities, allowing secure access to fees management features.

Fees communication	Communicates transparent, non-discriminatory, and proportionate fees provided by the system to make electronic health data available to data users. These fees are communicated transparently before the submission of the data access application or request.
Monitor application and permit status	Automatically tracks and maintains status updates of data access and request applications from submission to approval/refusal of requested data permits at the national level. Additionally, it automatically monitors the data permit until its expiry or the deletion of the dataset from the catalogue.
Fees management	Calculates and communicates transparent, non-discriminatory, and proportionate fees to make electronic health data available to data users. These fees will be communicated transparently before the submission of the data access application or request. Generates invoices to be paid when the data permit is generated.

Proposed services:

Following the CY-EHDS-2nd CP design principles we can consider the following microservices to support the domains' core features as outlined in Table 44.

- *Real-time cost estimator*: To provide fee estimation in real-time, calculating fees based on selected datasets and application input details, before the application is submitted.
- *Invoice microservice*: To calculate and generate invoices with detailed fee concepts, after data application submission or upon withdrawal, notifying data users about payment deadlines.
- *Payment processing*: To provide a secure payment process for the generated invoices, using a payment interface that supports multiple payment methods.
- *Compensation for data holders*: To calculate a compensation for the usage of their datasets and inform them about pending and completed compensations.

Integrations:

The system will facilitate interactions with data users for invoice payments. To ensure secure payment processing, data users will be required to utilize a platform specifically designed for this purpose.

4.2.3 Permits management

This section outlines the services for managing data permits, including the services involved in negotiating data permits and handling appeals in cases of permit refusals. This domain covers the processes related to data permit negotiation and appeals management, while also addressing security measures for user access, the signing of contract documents, and the payment of invoices associated with data permits.

Table 44: Permits Management Core Features

Feature/ service	Description
User IAA	Validates user identities, allowing secure access to permit management features. - Confirms user identity when managing appeals for revoked permits.

	- Confirms user identity when accessing to the data permit status dashboard. - Ensures secure access to permit negotiation, contract signing and amendment processes.
Allow for Data Access and Request Application Management	Manages data permits, from creation to issuing decisions, including documents such as contracts and invoices. - Displays the status of data permits in a dashboard, allowing user to review the status.
Monitors Application and Permit Status	Tracks the status of the data permits, including all relevant information attached to the data permit, that the data user can review. - Displays status updates in the dashboard of the data permits, allowing the user to review the information about the status. - Notifies users about any status change that the data permit receives.
Allows to Communicate Decisions	Notifies data users about the outcome decision of the data permit. - Communicates data permit and appeal decisions to the data user.
Fees Management	Calculates permit fees, communicating cost to the data user including this information in an invoice sent to the data user to review it. - Provides fee management for permit processing, invoicing data users after negotiation completion.

Proposed services:

Following the CY-EHDS-2nd design principles we can consider the following microservices to support the domains' core features as outlined in **Error! Reference source not found.**.

- *Data permit*: To manage data permit lifecycle, tracking the status and handling amendments.
- *Negotiation and Signature*: To facilitate contract negotiation, signature capture and persistence of signed documentation.
- *Payment processing*: To provide an invoice of the data permit related fees and facilitate the payment process to the data user.
- *Appeals microservice*: To manage appeal submissions and track the status of the submitted appeals to re-consider a data permit decision taken.

Integrations:

Payment Process:

The system will facilitate interactions with data users for invoice payments. To ensure secure processing, data users will be required to utilise a government platform for making payments.

5 PROTOTYPE

The design of the CY-EHDS-2nd HDAB Portal in terms of look and feel, will adhere to the national design principles of gov.cy[5] (Figure 7).

Figure 7: gov.cy unified design system

User authentication and authorization will be through the CY Login Figure 8.

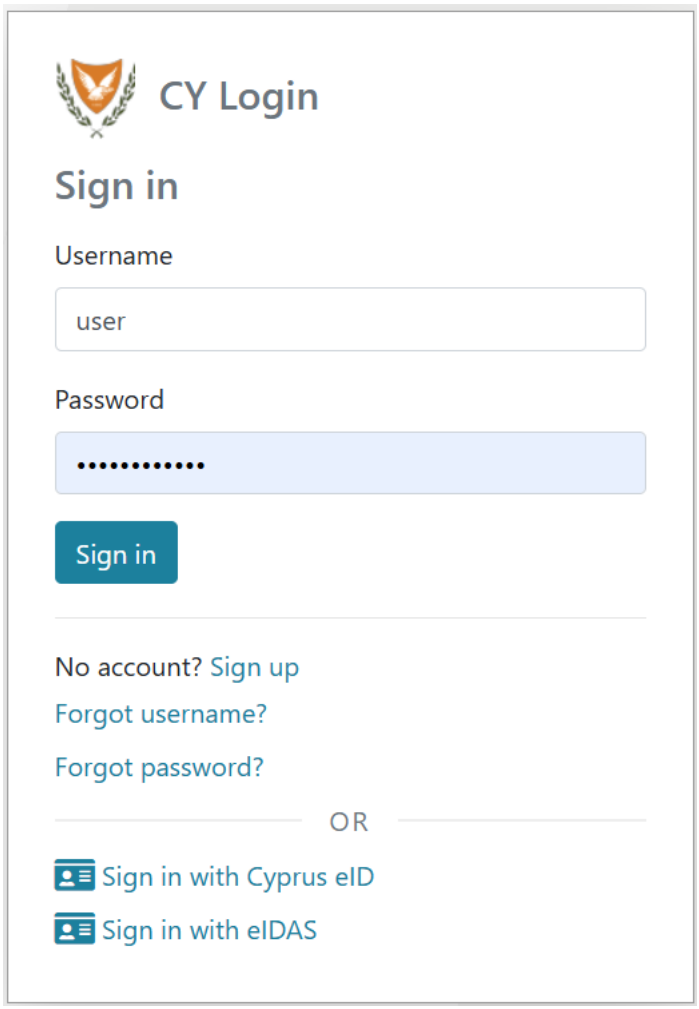

Figure 8:Cy Login

The Dataset Catalogue option will provide functionality for navigating / searching the national dataset catalogue, similar to the implementation of the EU Dataset Catalogue (Figure 9):

[5] https://gov-cy.github.io/govcy-design-system-docs/

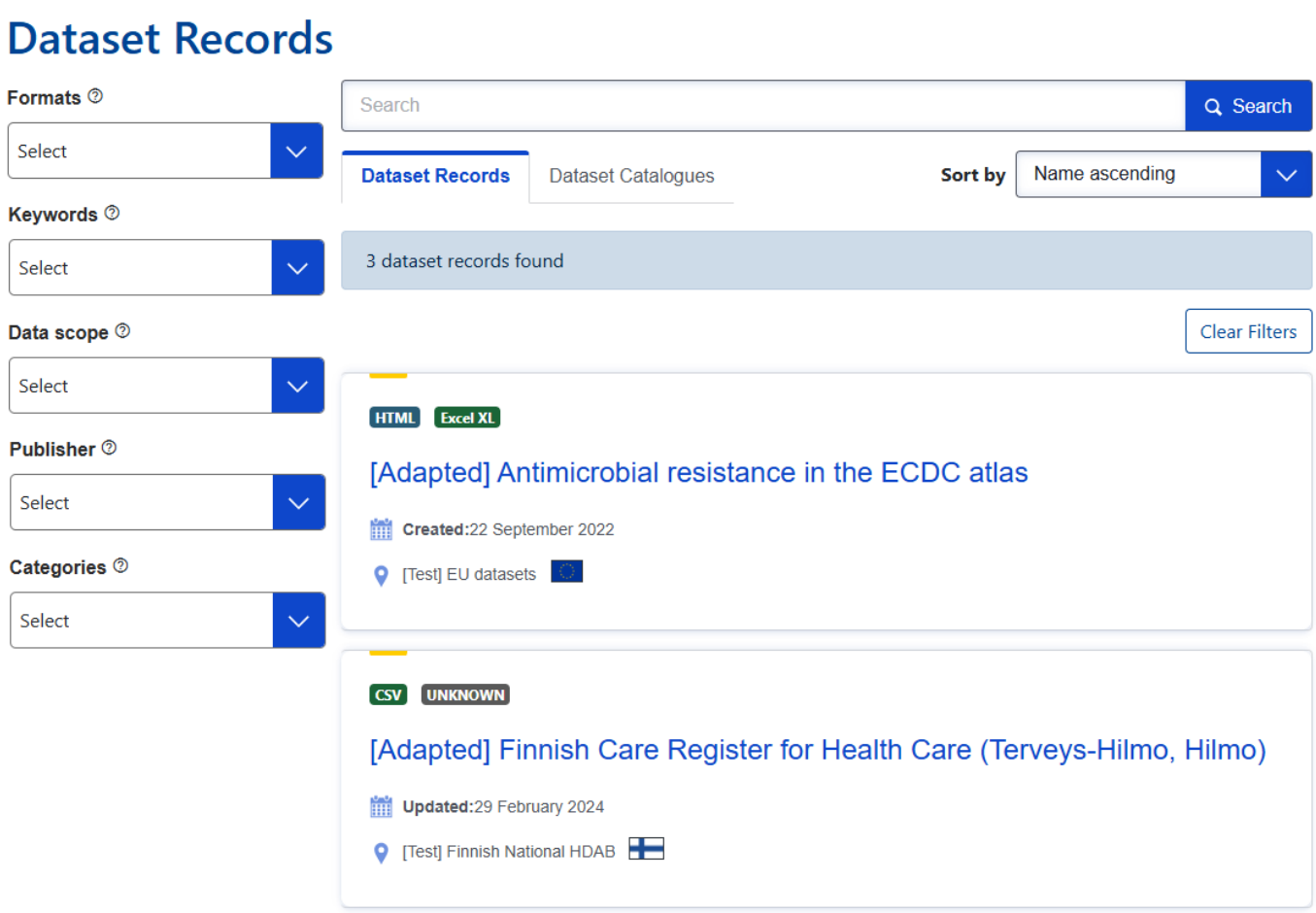

Figure 9: Dataset Catalogue Navigation / Search (HealthData@EU CP example)

The Applications menu will provide different links to Data Access Applications (Figure 10) and Data Request Applications (Figure 11) respectively. The options the system will display for each application in the dashboard will depend on the status of the application and the role (privileges) of the user.

Figure 10: Dataset Access Applications Dashboard (HealthData@EU CP example)

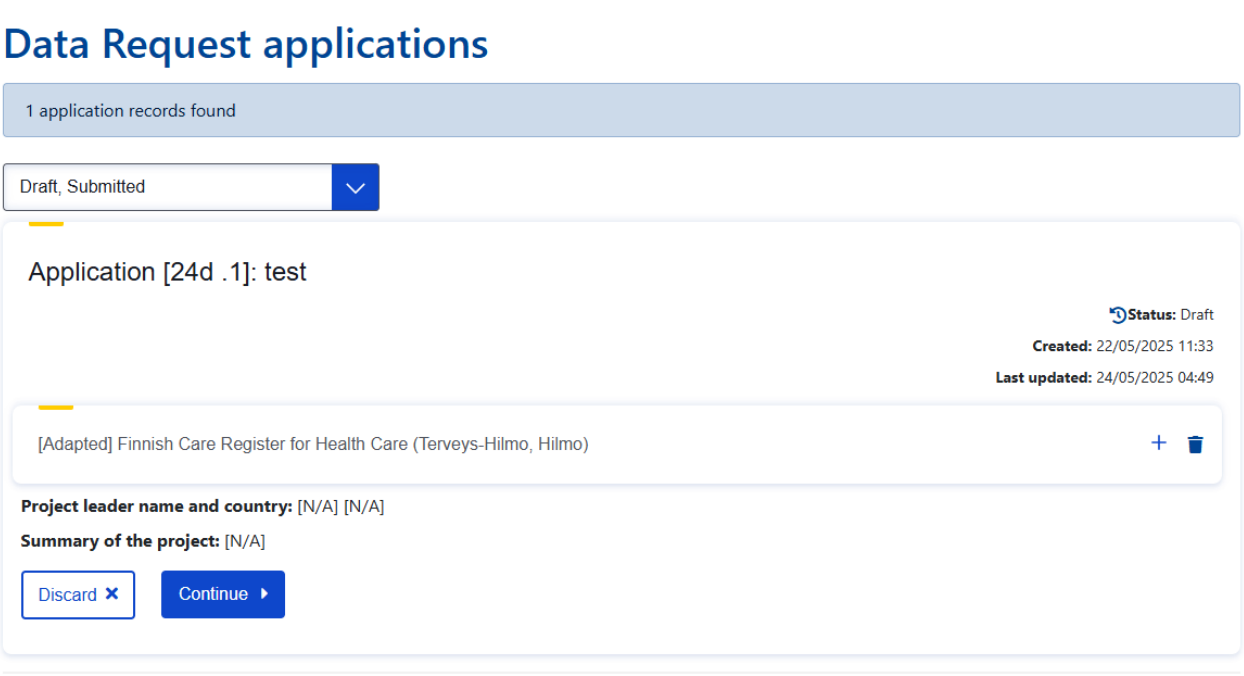

Figure 11 Dataset Request Applications Dashboard (HealthData@EU CP example)

The application forms will also be designed/ implemented following the common application forms of the HealthData@EU CP. The Data Permits management dashboard will also be designed and implemented following the same design principles.

6 REFERENCES

1 **European Commission, Directorate-General for Health and Food Safety (2025)**. *HealthData@EU Central Platform – Open-source Release 3: Objective, Business Requirements and Use Cases*. Luxembourg: Publications Office of the European Union, March 2025. ISBN: 978-92-68-26028-9. DOI: 10.2875/5437350.

2 **European Commission, Directorate-General for Health and Food Safety (2025)**. *HealthData@EU Central Platform – Open-source Release 3: Architecture Model and Technical Specification*. Luxembourg: Publications Office of the European Union, March 2025. ISBN: 978-92-68-26029-6. DOI: 10.2875/6472234.

3 **PwC EU Services (for DG SANTE) (2024)**. *Requirements Catalogue for Scale-Up Version (Deliverable D02.03)*. Specific Contract No. 022 under Framework Contract SLG.AVT.DI07926 – BEACON, Lot 2. European Commission, December 2024.

4 **PwC EU Services (for DG SANTE) (2024)**. *Architecture Artefacts – Scale-Up Version (Deliverable D03.03, Part 1: Architecture)*. Specific Contract No. 022 under Framework Contract SLG.AVT.DI07926 – BEACON, Lot 2. European Commission, December 2024.

5 **PwC EU Services (for DG SANTE) (2024)**. *System Specifications – Scale-Up Version (Deliverable D03.03, Part 2: System Specifications)*. Specific Contract No. 022 under Framework Contract SLG.AVT.DI07926 – BEACON, Lot 2. European Commission, December 2024.

6 **PwC EU Services (for DG SANTE) (2024)**. *Testing Framework – Scale-Up Version (Deliverable D03.03, Part 3: Testing Framework)*. Specific Contract No. 022 under Framework Contract SLG.AVT.DI07926 – BEACON, Lot 2. European Commission, December 2024.

7 **PwC EU Services (for DG SANTE) (2024)**. *ICT Governance Framework and Procedures Catalogue – Scale-Up Version (Deliverable D04.03)*. Specific Contract No. 022 under Framework Contract SLG.AVT.DI07926 – BEACON, Lot 2. European Commission, November 2024.

8 **European Parliament and Council of the European Union (2025)**. *Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847*. *Official Journal of the European Union*, L 2025/327, 5 March 2025. ELI: http://data.europa.eu/eli/reg/2025/327/oj

9 **TEHDAS2 (2025)**. *D6.3 Internal Draft Guideline for Health Data Access Bodies on the procedures and formats for data access*. TEHDAS2 Project, May 2025.

10 **TEHDAS2 (2025)**. *D6.4 Internal Draft Technical Specifications for Data Access Application Management System (DAAMS) for Health Data Access Bodies (HDABs)*. TEHDAS2 Project, May 2025.

11 **European Commission (2025)**. *Digital Business Capabilities Blueprint*. EHDS2 Community of Practice Confluence Page, January 2025.

ANNEX A - CY-EHDS-2ND ARCHITECTURE AND CP INFRASTRUCTURE

EXECUTIVE SUMMARY

The EHDS for Secondary Use @CY (CY-EHDS-2nd)[6] General Infrastructure annex defines the architectural, functional and technical foundations for the national platform supporting the secondary use of health data in the Republic of Cyprus, as mandated under the EHDS Regulation European Union (EU) 2025/327[7].

This infrastructure is coordinated by the National eHealth Authority (NeHA)[8], the designated Health Data Access Body (HDAB) of Cyprus and establishes a modular and standards-aligned environment for enabling secure, auditable and legally compliant health data access.

This document is provided as Annex A to D5.1 "Data Access Application Management System – Requirements and Specifications". While not submitted as a standalone deliverable, it serves the function of a horizontal deliverable by defining the common infrastructure architecture and central platform (CP) integration layer underpinning all five modules of the CY-EHDS-2nd infrastructure. Its role is to provide a unified architectural and technical foundation referenced by D5.1 through D9.1. It covers all shared infrastructure elements and cross-cutting services that support the five functional Work Packages (WP) (Data Access Applications Management solution (DAAMs), nHDsC, Secure Processing Environment (SPE), Cross-Border Gateway, Dataset Quality Enhancement Toolbox (DQET), which are described in separate documents.

The central focus is the Central Platform Layer (CPL), which provides common services for identity federation, access orchestration, role enforcement, accreditation routing and audit logging through four reusable Shared Services (CPSS1–CPSS4). It interfaces with national services such as CY Login and provides an access layer for both data users and data holders.

Additional supporting infrastructure includes:

- A shared observability stack used by all components
- A profile service for account lifecycle management
- An event bus for modular integration and event-driven traceability
- OpenAPI[9]-based Application Programming Interface (API) governance managed by NeHA

Annex A ensures full architectural alignment with HealthData@EU (CP) Release 3 documentation and relevant deliverables provided via the EHDS for the secondary use of health data (EHDS2) Community of Practice.

The document is intended for technical implementers and the governance authority (NeHA), and reviewers involved in evaluating or deploying the CY-EHDS-2nd system. It includes a full breakdown of functional and non-functional requirements (NFRs), technical specifications, and cross-references to module-specific deliverables.

[6] https://www.cy-ehds-2nd.eu/

[7] https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng

[8] https://www.neha.org.cy/

[9] https://www.openapis.org/

Table of contents

List of Tables

List of Figures

ANNEX A Abbreviations

AE	Affiliated Entity
2FA	two-factor authentication
ACLs	Access Control Lists
AE	Affiliated Entity
API	Application Programming Interface
AS4	Applicability Statement 4
CNIL	French data protection authority
COO	Coordinator
CP	Central Platform
CP R3	Central Platform Release 3
CPL	Central Platform Layer
CRUD	Create, read, update, and delete
CY-EHDS-2nd	European Health Data Space for Secondary Use @CY
DAAMs	Data Access Application Management solution
DGA	Data Governance Act
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DQET	Dataset Quality Enhancement Toolbox
DQUL	Dataset Quality and Utility Label
DQV	Data Quality Vocabulary
EC	European Commission
EHDS	European Health Data Space
EHDS2	European Health Data Space for the secondary use of health data
eID	electronic IDentification
ESPE	External Securing Processing Environment
EU	European Union
EU4H-JA	EU4Health-funded joint action
FAIR	Findability Accessibility Interoperability and Reuse of data
FRs	Functional Requirements
GDPR	General Data Protection Regulation
GIP	Public Interest Grouping
HDAB	Health Data Access Body
HDH	Health Data Hub
Health DCAT-AP	Health Data Catalogue Vocabulary Application Profile
IAA	Identification, authentication, and authorization
ID	Identification
ISPE	Internal Secure Processing Environment
ITB	Interoperability Test Bed
JSON	JavaScript Object Notation
JSON-LD	JavaScript Object Notation for Linked Data
MFA	multifactor authentication
MS	Member States
mTLS	mutual Transport Layer Security

NCP	National Contact Point
ND	National HealthData@EU Dispatcher
NeHA	National eHealth Authority of Cyprus
NFRs	Non-Functional Requirements
nHDsC	National Dataset Catalogue for health data
NRO	Non-Repudiation of Origin
NRR	Non-Repudiation of Receipt
PMode	Processing Mode
RBAC	role-based access control
RDF	Resource Description Framework
REST	Representational State Transfer
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SFTP	Secure File Transfer Protocol
SHACL	Shapes Constraint Language
SLA	Service Level Agreement
SOAP	Simple Object Access Protocol
SPE	Secure Processing Environment
TEHDAS2	Second Joint Action Towards the European Health Data Space
TLS	Transport Layer Security
UCP	Union Contact Point
UCY	University of Cyprus
UDAS	Union Data Access Service
VM	Virtual Machine
WP	Work Package
WS	Web Service
XBDE	Cross-Border Data Exchange
XBG	Cross-Border Gateway
XML	eXtensible Markup Language

A.1 INTRODUCTION

This annex presents the overall architecture of the CY-EHDS-2nd infrastructure and introduces its functions and capabilities. It provides a high-level vision of the system's structural design and its role within a broader EU eHealth ecosystem by supporting secure, efficient and legally compliant access to health data for secondary purposes such as research, innovation, public health monitoring and evidence-based policymaking. The CY-EHDS-2nd infrastructure is composed of five main components:

1. The nHDsC
2. The DAAMs
3. The SPE
4. The National Connector for Cross-border gateway
5. The Health Data Quality Enhancement (HDQE) Toolbox

The architecture is built on four foundational principles:

1. Full alignment with the EHDS Regulation [8]
2. Adequate implementation of the relevant EHDS2 Digital Business Capabilities (DBCs) [9]
3. Interoperability with the HealthData@EU CP[10], including reusing, where feasible, components and patterns of the existing European solution [1-2]
4. Future readiness, allowing for continuous adaptation and enhancement as new deliverables from EU initiatives such as Second Joint Action Towards the EHDS (TEHDAS2[11], QUANTUM[12] and the forthcoming EHDS2 implementing acts become available.

While this annex provides the overarching architecture for the CY-EHDS-2nd solution, laying out the conceptual framework that inspired and shaped its design, more detailed analysis of each infrastructure component will follow in separate deliverables (D5.1 to D9.1). Each of these will focus on the business requirements and technical specifications of one specific module of the system:

- D5.1 – DAAMs Requirements, Specifications and Prototype
- D6.1 – nHDsC Requirements and Specifications
- D7.1 – SPE Requirements and Specifications
- D8.1 – National Connector for Cross-border gateway Requirements and Specifications
- D9.1 – Health data quality enhancement toolbox Requirements and Specifications

In the context of this document, particular emphasis is given to the CPL (CY-EHDS-2nd CP), which serves as the core coordinating component of the national infrastructure for secondary use. The CY-EHDS-2nd CP is introduced as the backbone of the architecture, responsible for securely orchestrating interactions between all key national modules: the nHDsC, the DAAMs, the SPE, the NCP for cross-border cooperation and the dataset quality enhancement. This central coordination capability ensures consistent workflows, streamlined data access procedures, and full interoperability across both national and European levels.

Beyond its current scope, the platform is designed as a living system able to support not only its initial rollout but also its long-term evolution. Its structure is modular and adaptable, enabling ongoing refinement, scaling and alignment with emerging EU-wide initiatives and governance updates.

Looking ahead, the CY-EHDS-2nd CP, together with the planned Single Electronic Health Record Data Bank (SeHRB) of Cyprus, is envisioned as the cornerstone of a connected national eHealth ecosystem. By bridging primary and secondary use of health data, this ecosystem will promote more holistic, person-centred care and contribute to the long-term resilience and effectiveness of the national health system, ultimately supporting the well-being of all citizens in Cyprus.

A.1.1 Target Audience

This document addresses the needs of the following audiences:

A. System Architects and Engineers: This document serves as a core reference for system architects and engineers tasked with implementing and maintaining the CY-EHDS-2nd infrastructure. These professionals must interpret and apply the system's architectural design, component specifications, and integration patterns in practice. Given that the infrastructure will evolve over time through iterative releases, it is essential that system architects and engineers operate with a consistent and

[10] https://acceptance.data.health.europa.eu/
[11] https://tehdas.eu/
[12] https://quantumproject.eu/

aligned understanding of the system's structure, design principles and component interactions. This document is intended to support that continuity and shared vision across all stages of the system's development and lifecycle.

B. Developers: This document provides developers with clear insights into the architectural guidelines, integration points and system design constraints of the CY-EHDS-2nd infrastructure. By aligning their development activities with the architectural standards outlined herein—particularly those related to modularity, interoperability and cloud-native deployment—developers can ensure code-level compliance and optimise application performance across environments.

C. Development, Security and Operations (DevSecOps) teams: This audience may reference this document to gain a structured understanding of the system's architecture, component responsibilities and deployment models. It supports infrastructure-as-code practices, secure configuration management and operational readiness by outlining how different modules interact and the compliance requirements associated with running the CY-EHDS-2nd infrastructure in a secure and scalable way.

A.1.2 Legal Framework

The CY-EHDS-2nd infrastructure is developed within a legal framework that ensures the secure, lawful, and trustworthy secondary use of health data. This framework combines European-level regulations with national legislation, forming the legal backbone that governs the secondary use of health data infrastructure operations, its interoperability with the HealthData@EU CP and its alignment with the rights of the citizens.

At the core of this framework is Regulation (EU) 2025/327 on the EHDS [8], which lays down common rules for the secondary use of electronic health data across all EU Member States. The regulation introduces a structured governance model, clearly identifies the roles of national authorities as the HDABs, data holders, and data users and sets strict conditions under which health data can be reused for purposes like research, policymaking, innovation, or public health planning. The CY-EHDS-2nd infrastructure plays a central role in enabling Cyprus to meet these obligations, both at national level and within the wider HealthData@EU ecosystem.

Importantly, the General Data Protection Regulation (GDPR)[13] remains fully applicable in this context. The EHDS builds on the GDPR strong data protection principles such as data minimisation, purpose limitation, and rights of individuals while adding specific provisions for pseudonymisation, access control and oversight tailored to the reuse of sensitive health data. The technical and organisational measures embedded in the CY-EHDS-2nd infrastructure must meet these dual legal requirements.

In addition to the EU framework, Cyprus has its own national law regulating eHealth systems and the management of health data at national and cross-border level, enacted in 2019. One of its core provisions was the establishment of NeHA as the competent authority for overseeing national eHealth infrastructure.

While the national eHealth law in Cyprus[14] provides extensive and detailed provisions for the primary use of electronic health data, its references to secondary use remain limited in scope and specificity. In particular, the law does not yet clearly define the roles, responsibilities, or processes associated with secondary data access, nor does it establish a legal foundation for the supporting infrastructure components required under the EHDS framework. NeHA, as already established under the 2019 law, has been designated as the single

[13] https://gdpr-info.eu/

[14] https://www.neha.org.cy/en/legislation/

HDAB in accordance with Article 55 of the EHDS Regulation and is responsible for implementing all tasks associated with the national infrastructure for secondary use.

In preparation for the legal and operational alignment with EHDS, NeHA is currently conducting a comprehensive impact assessment to analyse the implications of the regulation on the national health data landscape. The outcome of this assessment will guide the formulation of legislative amendments and the design of associated institutional procedures. Legislative updates are anticipated in 2026 to formally address current gaps and ensure full alignment with the structured governance model, safeguards and interoperability requirements defined by the EHDS.

Looking ahead, the EC is preparing a series of implementing acts, which are scheduled to be adopted by March 2027. These acts will provide further detail on key aspects of the EHDS framework, including technical standards, interoperability protocols, data quality rules and secure processing requirements. Once adopted, Cyprus will integrate these implementing acts into its national legal and operational framework, ensuring the platform remains aligned with evolving European standards and is prepared to support future cross-border services.

Concluding, the legal foundation of the CY-EHDS-2nd infrastructure is built to evolve. It reflects both current obligations and forward-looking developments, ensuring the platform operates within a trusted, rights-based and future-proof legal environment at both national and EU level.

A.1.3 Related projects

In response to the proposal and enactment of the EHDS, the EU has launched a series of strategic projects aimed at supporting Member States in implementing the regulation's provisions. These projects not only offer essential policy guidance and technical specifications but also develop key enabler such as common standards, interoperable tools and data governance models that can be leveraged by national implementations.

For the Republic of Cyprus, the design and development of the CY-EHDS-2nd infrastructure have been directly informed by the outputs of three major European projects: HealthData@EU Pilot[15], TEHDAS2 and QUANTUM. These projects serve as foundational references, offering architectural models, specifications, and evolving guidelines that are being adapted to the national context as part of a living design process. Their relevance is continuously assessed throughout the development lifecycle of CY-EHDS-2nd, ensuring ongoing alignment with the EHDS Regulation and readiness for cross-border integration.

A.1.3.1 HealthData@EU pilot

Duration: October 2022 – September 2024 | Funding: EU4Health Programme

HealthData@EU pilot was one of the earliest projects targeting the secondary use of health data at EU level [10]. Coordinated by the French Health Data Hub and implemented by a consortium of 17 partners across Member States, its core mission was to design, build and test a federated infrastructure enabling cross-border data access for secondary use in line with the EHDS vision.

Several of the project's outputs have been directly utilised in the early architecture and requirements definition of the CY-EHDS-2nd infrastructure which are outlined in Table A. 1.

Table A. 1: HealthData@EU pilot deliverables related to CY- EHDS-2nd

[15] https://ehds2pilot.eu/

Deliverable	Related to CY-EHDS-2nd
D5.1 Architecture Definition Document	CP
D6.1 HealthData@EU pilot project - Deliverable 6.1 Extension of Data Catalog Vocabulary Application Profile (DCAT-AP): Health DCAT-AP[16] The extension of DCAT-AP, known as Health DCAT-AP, is a metadata standard specifically designed to support the description of health datasets intended for secondary use. The project delivered a draft version of this standard to TEHDAS2, which will finalise it and establish it as the core metadata standard for exchanging dataset record descriptions within the HealthData@EU CP.	WP 6
D7.1 Common data access application forms to boost cross-border use of electronic health data within the EU	WP5, WP8
Deliverable 8.2 Recommendations on quality controlling, assurance & provenance	WP9

Part of this project's work was leveraged for the design and implementation of the Healthdata@EU CP infrastructure while some results have also been passed on to TEHDAS2 for further refinement, with the intent of feeding into the upcoming EHDS implementing acts.

A.1.3.2 TEHDAS2

Duration: May 2024 – December 2026 | Funding: EU4Health Programme (Joint Action Instrument)

TEHDAS2 is the official successor to the first TEHDAS Joint Action [11]. Building on the deliverables of its predecessor and the HealthData@EU pilot, it aims to support the practical implementation of the EHDS Regulation across Europe and more particularly by HDABs, data holders and secondary data users.

The consortium brings together a broad range of partners from EU Member States. Its deliverables include both technical specifications and operational guidelines, many of which are expected to inform the EC's forthcoming EHDS implementing acts.

Although TEHDAS2 key outputs will be delivered after the finalisation of the CY-EHDS-2nd requirements phase, they will be closely monitored and integrated wherever relevant in future updates. The most critical deliverables relevant to CY-EHDS-2nd infrastructure are presented in Table A. 2.

Table A. 2: TEHDAS2 related deliverables to CY- EHDS-2nd

Deliverable	Due to	Related to CY-EHDS-2nd
D7.3: Technical specification for HDABs on the implementation of the common Information Technology (IT) infrastructure	February 2026	CP
D6.3: Guideline for HDABs on the procedures and formats for data access	February 2026	WP5
D6.4: DAAMs - Technical specification for HDABs	October 2026	WP5

D5.1: Guideline for data holders on data description	July 2025	WP6, WP9
D5.2 Guidelines for HDABs on minimum categories and limitations on the reuse of health data	March 2026	WP6, WP9
D5.3 Technical specification for HDABS on the national metadata catalogue	July 2025	WP6, WP9
D6.1 Guideline for data holders on making personal and non-personal electronic health data available for reuse	February 2026	WP6, WP9
D7.2: Technical specification for HDABs on data minimization and de-identification	February 2026	WP7
D7.4: Technical specification for HDABs on the implementation of SPEs	September 2026	WP7
D4.2: Guideline for HDABs on collaboration with other parties	October 2026	WP8
D4.3: Guideline for HDABs on international and third-country access and transfer of personal and non-personal electronic health data	October 2026	WP8

As part of a living design process, CY-EHDS-2nd will incorporate updates and refinements based on these deliverables to ensure full compliance with evolving EHDS norms and consistency with EU-wide practices.

A.1.3.3 QUANTUM

Duration: February 2024 – January 2027 | Funding: Horizon Europe – Research and Innovation Action

QUANTUM is a research project focused on improving data quality and trust in the secondary use of health data within the EHDS ecosystem [12]. The project's ambition is to create a usable and standardised data quality labelling system for HDABs and data holders across Europe.

The deliverables of this project are focused in:

- Data Quality labelling system
- Maturity Assessment Framework
- Pilot Implementations

From which the most related deliverables to CY-EHDS-2nd are presented in Table A. 3.

Table A. 3: QUANTUM deliverables related to CY- EHDS-2nd

Deliverable	Due to	Related to CY-EHDS-2nd
Deliverable 1.1 Specification of the data sets' quality and utility label	February 2025	WP9

These outputs are expected to help CY-EHDS-2nd to establish a structured approach for assessing dataset quality and institutional readiness. Through the implementation of our WP9 we will incorporate these standards to ensure that the datasets made available via the national infrastructure for the secondary use

of health data are transparent, reliable and fit for purpose and thereby enhancing their usability and trustworthiness for data users.

A.1.4 EHDS journey for secondary use

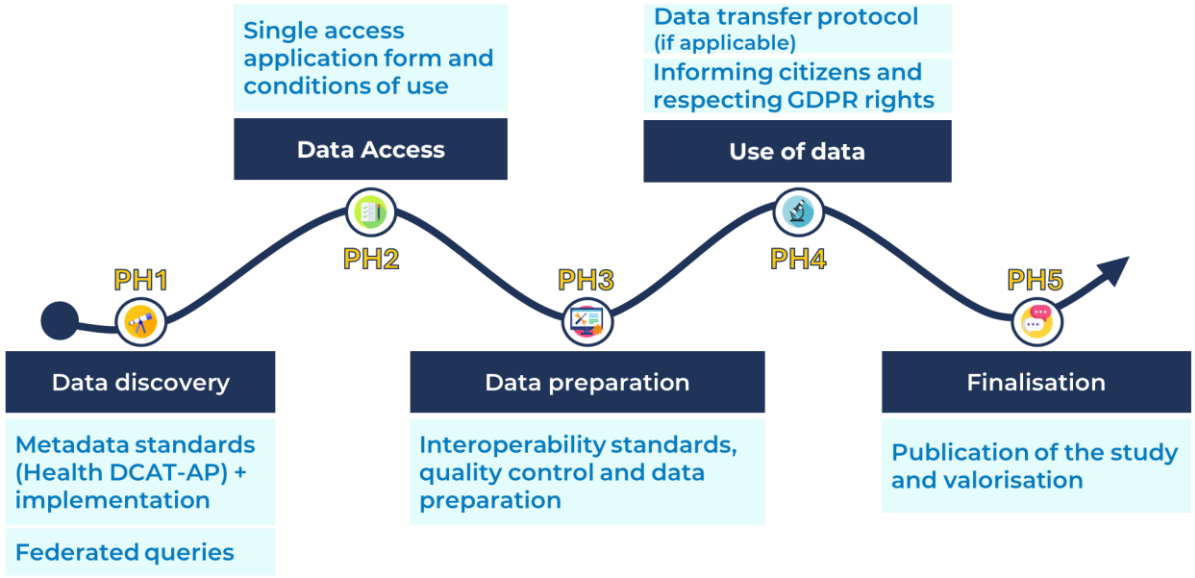

Figure A. 1: The EHDS data user journey for secondary use of health data, as proposed by the HealthData@EU pilot project and adopted by the TEHDAS2 project, can be divided into five distinct phases, labelled PH1 through PH5.

The EHDS2 data user journey outlines the end-to-end process through which a data user (e.g. a researcher, policymaker, innovator or public health body) interacts with the infrastructure to gain lawful and secure access to electronic health data for secondary use. This journey, first conceptualised in the HealthData@EU pilot project [10] and now formally adopted by TEHDAS2 [11] as a guiding framework, is structured around five core phases which are presented in Figure A. 1 and are described in Table A. 4.

Within the CY-EHDS-2nd project, the EHDS2 data user journey has been adopted as a central reference to ensure consistency with the European data user's experience expectations. Each of the national components, the nHDsC, DAAMs, SPE, Cross-border Gateway and the Quality Toolbox, are designed to align with the logical steps and decision points of this journey. This approach ensures that the Cypriot infrastructure for the secondary use of health data is both user-oriented and interoperable with the broader HealthData@EU ecosystem.

Table A. 4: EHDS2 health data user journey phases

Phase	Name	Description	CY-EHDS-2nd alignment
PH1	Data Discovery	Users search for datasets relevant to their needs through a federated catalogue interface. They can filter their search using various criteria and view each dataset's standardised metadata, structured according to the Health DCAT-AP profile, along with any associated quality labels. These elements help assess the dataset's fitness for the intended secondary use. This phase is designed to be transparent and efficient, allowing users to quickly identify suitable datasets and understand any applicable access conditions or limitations.	**CP, WP6, WP8, WP9** This phase is supported by the nHDsC which connects to the HealthData@EU CP catalogue providing all the national metadata records through the NCP and eDelivery network.
PH2	Data Access	Once users have identified the datasets they wish to access, they proceed to prepare and submit a data access application. This application is routed through the HDAB, where it undergoes a formal evaluation process. Based on this assessment, the HDAB may issue a positive decision by granting access through a data permit or providing aggregated data through a data request, or a negative decision, in which case the application process is concluded.	**CP, WP5, WP8** This functionality is managed by the DAAMs, developed under WP5 and integrated through the CP. In the case of a positive evaluation (resulting in a data permit or data request), the CP enables the connection to the relevant permit management components. Additionally, it facilitates the exchange of applications received from the HealthData@EU CP, as well as the transmission of evaluation outcomes, whether positive or negative, back to the originating system. This integration supports the coordination across national and cross-border access workflows, aligning with the objectives of WP8.
PH3	Data Preparation	After the application is submitted and approved, the process enters the data preparation phase. During this phase, the data holder makes the requested dataset(s) available, while the HDAB ensures the data is prepared for delivery in accordance with the authorised secondary use purpose. This preparation may involve steps such as	**WP7** This phase is supported by the internal SPE which will be provided by WP7. The internal SPE enables data holders to securely upload the requested datasets and provides the HDAB with controlled access to prepare the data in

		pseudonymisation, data transformation, merging of multiple data sources, or aggregation depending on the specific requirements of the application.	accordance with the approved secondary use purpose. In the case of a data permit, the prepared dataset is made available to the data user within their designated SPE. For data requests, the resulting aggregated data output is compiled and transmitted to the user via secure email.
PH4	Use of Data	Once authorised, the data user is granted access to the dataset via a SPE. The data is not exported or downloaded, instead users log in to a virtual environment where they can perform the desired analysis.	**WP7** The SPE for data users will be developed as part of WP7 providing a secure, access-controlled virtual environment in alignment with EHDS enforcing strict data protection and access control mechanisms ensuring that no personal data can be exported, downloaded or transferred outside the environment. It will offer technical tools for statistical analysis, modelling and output review.
PH5	Finalisation	The final phase of the EHDS2 data user journey is marked when the data permit expires according to the terms defined in the authorisation. Once expired, the data user must cease all processing activities associated with the permit. Health data within the SPE must be deleted within six months of the data permit expiry, under the responsibility of the HDAB. Furthermore, the data user is required to inform the HDAB of any outputs resulting from the data use. These results must be made publicly available within 18 months after processing is completed and must clearly acknowledge that the data were accessed through the EHDS framework.	**CP, WP5, WP7** The management of data permit expiration and post-processing obligations is handled through the Data Permit Management component of the CP, which is developed under WP5. This component oversees and controls the operation of the data user's SPE, delivered through WP7, ensuring that data processing is terminated in accordance with the validity conditions of the permit. Any required communication between the data user and the HDAB regarding the outcomes of the data analysis is facilitated via secure email channels.

A.1.5 HDAB Digital Business Capabilities

To support Member States in understanding and implementing the organisational and technical responsibilities of HDABs under the EHDS, the EC has developed a set of DBCs [9]. These capabilities provide a conceptual model that captures the key information flows, decision points and functional requirements that HDABs are expected to manage at both national and cross-border levels. It is important to clarify that the HDAB DBC framework is not legally binding, nor does it impose any specific technical solution or infrastructure. Instead, it serves as a practical blueprint, offering guidance and shared understanding of the business domains that HDABs must address to comply with EHDS obligations and to enable efficient and interoperable data access services. **Error! Reference source not found.** depicts the HDAB DBC blueprint in a v isual diagram as shared and presented by the Commission (available on the EHDS2 Community of Practice Confluence page[16]). Each capability in the model is represented as a functional "box" and illustrates a distinct area of information management. The links between capabilities depict the logical flow of data or control messages, rather than the implementation method. Member States retain full flexibility in how they implement each capability, according to their national context, digital maturity, legal landscape and organisational models. Whether implemented via dedicated software, secure email exchanges, manual workflows, or more advanced digital platforms, what matters is that the core information functions are fulfilled, not how they are technically realised.

For Cyprus, the HDAB DBC framework is used in two main ways:

1. As a design support tool, to help structure and define the CY-EHDS-2nd infrastructure components and their interactions, ensuring full coverage of the corresponding HDAB functions presented per each DBC in the blueprint.
2. As a communication and coordination tool, allowing various stakeholders to develop a common understanding of the infrastructure's expectations, workflows and responsibility areas, regardless of their technical background.

Importantly, not all HDAB DBCs are of equal status:

- Some capabilities are mandatory, as they correspond to explicit legal requirements under the EHDS regulation.
- Others are recommended, meaning that while not legally required, their implementation is encouraged to ensure better coordination and interoperability across Member States.

In the official HDAB DBCs blueprint (Figure A.2), mandatory DBCs are marked with a red dot. Each DBC is further broken down into atomic actions, which represent the specific functions or operations the HDAB must enable. The diagram also identifies actors who are depicted with human-shaped icons. The actors describe who are authorised or required to interact with each capability.

Within CY-EHDS-2nd, several DBCs, both mandatory and optional, are addressed across WP5 through WP9. However, not all mandatory HDAB DBCs will be implemented directly through this project and therefore complementary efforts will be required to fully meet EHDS obligations and complete functional coverage of the HDAB of Cyprus.

The full list of HDAB DBCs, including their description, interdependencies with other DBCs, mandatory status and their relevance to CY-EHDS-2nd, is provided in ANNEX B.

[16] https://webgate.ec.europa.eu/fpfis/wikis/pages/viewpage.action?spaceKey=EHDS&title=COMMUNITY+OF+PRACTICE

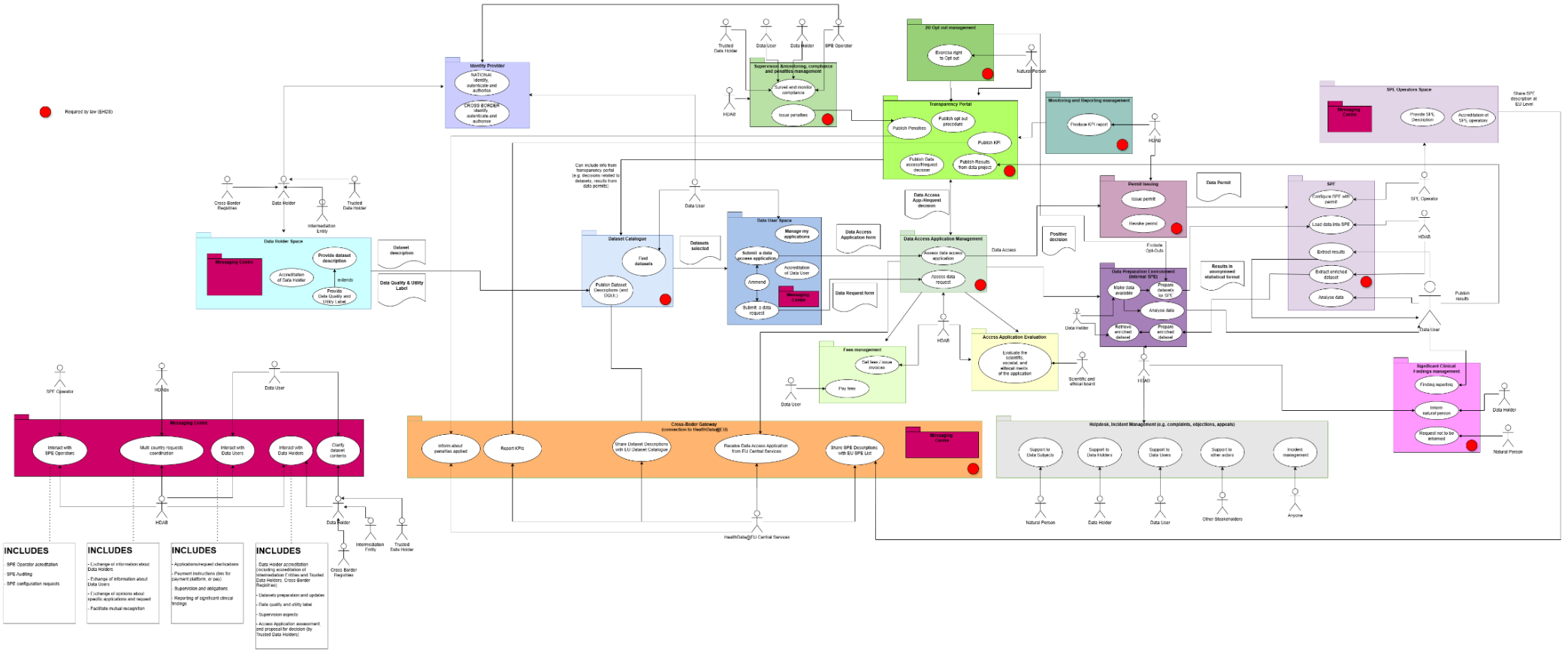

Figure A. 2: The diagram presenting HDAB BDCs blueprint as provided by EC

A.1.6 HealthData@EU Infrastructure and Central Platform

The HealthData@EU infrastructure is the official cross-border framework enabling the secondary use of electronic health data across the Union, as defined in Article 75 of the EHDS regulation [8]. It is a federated digital ecosystem that connects the NCPs for secondary use of each Member State with a centrally operated platform provided by the EC.

The purpose of this infrastructure is to support data users, such as researchers, policy makers, regulatory bodies and innovators, in accessing health data across borders under common rules, technical specifications and governance conditions.

A.1.6.1 HealthData@EU Infrastructure

According to Article 75(1–3) of the EHDS regulation, each Member State must designate a NCP for secondary use, aligned with its HDAB. These contact points:

- Act as organisational and technical gateways
- Enable and manage the cross-border availability of electronic health data
- Connect to the HealthData@EU infrastructure

The infrastructure includes:

- The NCPs and their own national HDAB infrastructure aligned with the EHDS regulation, including components such as dataset catalogues, DAAMs, SPEs and cross-border gateways.
- The Union health data access service (as the EU-level contact point for Union institutions).
- The HealthData@EU CP developed and operated by the Commission which enables cross-border interoperability at the technical, semantic and operational levels.

It is governed under a model where the Commission operates the platform as a processor, while NCPs retain the role of joint controllers over the processing activities in which they are involved.

A.1.6.2 HealthData@EU Central Platform

The HealthData@EU CP is a central interoperability and coordination layer hosted by the EC [1-2]. It enables cross-border cooperation between HDABs and ensures the consistent application of the EHDS regulation across the EU.

The HealthData@EU CP offers the following core functions:

1. **EU Dataset Catalogue:**
    - Aggregation of national and union dataset catalogues.
    - Compiled from metadata made available by data holders.
    - Publicly available and searchable information.
2. **Application Management (for Data Permit and Data Request):**
    - Submitting applications for data access and data requests using a single application form.
    - Monitoring the status of submitted applications.
    - Receiving the decision to the submitted application.

3. **Information Publication & Reporting:**
    - Publishing results or output of the secondary use of electronic health data.
    - Publishing information on Sanctions and Penalties.
    - Allowing HDABs to submit:
        - Biennial reports.
        - Information about all granted and revoked permits.
        - Information about applied penalties.
4. **User Management (Identification (ID), Authentication, and Authorisation):**
    - Services to identify, authenticate and authorize users before they can access restricted functionalities like application submission.
5. **Statistics Services:**
    - Publicly available statistics for the Dataset Records on the Platform (e.g., "Current state" and "Evolution over time").
6. **Platform Monitoring and Logging Services:**
    - Includes the resource and performance monitoring, the definition, management, and reporting of Key Performance Indicators (KPI) and the provision of dashboards for real-time visibility and operational insights.
7. **Search Functionality:**
    - Allows users to search the publicly available information (Dataset Catalogue, results, sanctions).
    - Includes SPARQL Protocol and Resource Description Framework Query Language (SPARQL) search capabilities for querying dataset records.

The technical design and operational logic of the platform, including interfaces, security protocols, and flow patterns, are detailed in the Release 3 documentation[17][1-2]. This release represents the most mature and consolidated version of the HealthData@EU CP specification to date and serves as the reference for Member States.

A.1.6.3 Relevance to the CY-EHDS-2nd Infrastructure

Cyprus, through the CY-EHDS-2nd project, is establishing its national infrastructure for the secondary use of health data entirely from scratch. Given the absence of an existing national framework, the project's strategic approach is to align fully with the HealthData@EU infrastructure and the CP model developed by the EC.

To achieve this, the CY-EHDS-2nd architecture:

- Adopts the HDAB DBCs blueprint.

[17] https://code.europa.eu/healthdataeu

- Structures national components (DAAMs, Dataset Catalogue, SPE, etc.) to mirror the EU-level interoperability model.
- Bases where applicable its business requirements and technical specifications on the finalized design of Release 3 of the CP.
- Where the HealthData@EU Central Platform R3 documentation [1–2] does not provide implementation-level detail, the design choices are guided by SC022 deliverables commissioned by the European Commission, DG SANTE [3–7].
- Intends to adapt the European solution as fully as possible, thereby avoiding duplication of design efforts and ensuring regulatory and technical consistency.

The Release 3 documentation has proven highly suitable to the needs and constraints of CY-EHDS-2nd. As a result, it will play a vital role in guiding both the drafting and refinement of national business requirements, not only during the design phase but also during pilot implementation, which will serve to validate interoperability with the EU infrastructure and prepare for subsequent CP releases.

This table-driven, standards-aligned strategy ensures that Cyprus can integrate effectively into the HealthData@EU ecosystem while building a robust, future-proof national system that does not reinvent functionalities already developed and validated at the European level.

A.2 CY-EHDS-2ND

A.2.1 Requirement Descriptors

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 CY-EHDS-2nd infrastructure, when something is described as "MUST," it means that the system must comply with the specific technical or security requirement for meeting EHDS and GDPR regulations. 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 CY-EHDS-2nd infrastructure documentation states that something "MUST NOT" occur, at 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 CY-EHDS-2nd infrastructure, when something is described as "SHOULD," at is highly advised but not strictly mandatory. For example, "The system SHOULD support multi-factor authentication (MFA) to enhance security."

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

4. MAY: This word, or the adjective "OPTIONAL", means that the item is truly optional. One vendor may choose to include the item because at enhances functionality, while another may omit it. In CY-EHDS-2nd

infrastructure, "MAY" is used to specify features or behaviours that are optional. For example, "The system MAY provide users with personalized notifications on data access events."

A.2.2 Target Architecture

The CY-EHDS-2nd platform will implement a modular and standards-aligned architecture, designed to enable the secure, interoperable and legally compliant secondary use of health data in Cyprus and across the EU. This section provides a high-level description of the national architecture and its alignment with the HealthData@EU CP reference model, as outlined in HealthData@EU CP Release 3 documentation while ensuring alignment with EHDS regulation.

A.2.3 System Architecture Overview

This section presents the unified architecture of the CY-EHDS-2nd infrastructure, combining both the design principles and the realised system layout. The CY-EHDS-2nd platform is implemented as a modular, containerised system deployed on a shared, Kubernetes-based national hosting environment. It enables secure, orchestrated and auditable access to health data for secondary use, under the governance and operational control of NeHA.

A.2.3.1 Architectural Design Principles

The CY-EHDS-2nd system adheres to the following foundational architecture principles:

- Modular Microservices Architecture: All components are designed as independent services, allowing for isolated deployment, scalability and lifecycle management.
- Centralised Session and Access Orchestration: The CPL, introduced in Section A.2.3.2, manages all user-facing sessions, enforces accreditation-based access controls and routes requests securely to internal services.
- Strict Separation of Responsibilities: While CPL handles identity, session, and access routing, business logic and data workflows remain within the respective functional modules (e.g. DAAMs, nHDsC).
- Shared Infrastructure Platform: All modules are deployed in namespaces on a shared Kubernetes environment maintained under national eHealth operations.
- Auditability and Traceability: All workflows, identity transitions, and access decisions are logged immutably and propagated to a shared observability backend.
- Compliance-Driven Design: The architecture complies with the EHDS regulation, the GDPR and the Cyprus eHealth Law.

A.2.3.2 Overall System Layout

The CY-EHDS-2nd infrastructure consists of five core functional modules and a set of shared platform components that are orchestrated centrally by the CPL. Each module provides distinct capabilities related to the secondary use of health data, while relying on centrally managed services such as identity, session management, observability and access control.

All modules are governed and operated by NeHA and will be hosted on the national Kubernetes-based infrastructure. Each core module (except the SPE) operates in isolation within its own Kubernetes namespace, with network policies enforced to ensure runtime isolation, independent deployment pipelines and security boundaries. The SPE is hosted as a logically isolated secure environment under NeHA control, following stricter access and execution policies.

Each of the five core modules is developed under a dedicated WP (WP5–WP9). These are summarised in Table A. 5.

Table A. 5: CY-EHDS-2nd core functional modules

Module	Description	CY-EHDS-2nd WP
DAAMs	Supports submission, triage, evaluation and coordination of data access applications and data requests by the HDAB (NeHA).	WP5
nHDsC	A structured repository of dataset metadata aligned with DCAT-AP and Shapes Constraint Language (SHACL) profiles, supporting dataset discovery by data users.	WP6
SPE	A protected infrastructure where permitted data users can access and analyse datasets under strict technical, legal and organisational controls.	WP7
National Connector and Cross-border Gateway	Can be analysed into two sub-components: (1) The national HealthData@EU dispatcher handling the orchestration, packaging, and dispatching of cross-border messages (applications, permits, datasets, etc.) with other Member States. (2) The cross-border gateway which is an interface component ensuring secure eDelivery and interoperability with the EU-level HealthData@EU Gateway, implemented using the Domibus framework.	WP8
DQET	A set of services and tools to assess, annotate and improve dataset quality and utility, including the application of labels as proposed by the project QUANTUM.	WP9

In addition to these functional modules, the CY-EHDS-2nd platform includes shared infrastructure layers that provide foundational technical services across the entire system. These components, presented in Table A. 6, are critical for interoperability, platform security and maintainability. They form the technical backbone of the CY-EHDS-2nd infrastructure, ensuring cohesive and standards-aligned operations across all modules although they do not deliver business capabilities in isolation.

Table A. 6: CY-EHDS-2nd platform shared infrastructure layers

CY-EHDS-2nd Shared Infrastructure Layer	Description
CPL	The national orchestration and access layer responsible for identity federation (via CY Login), user account management, accreditation enforcement, session handling and secure request routing to DAAMs, nHDsC, DQET and SPEs. CPL also provides logging and audit generation.
Shared Observability Stack	All modules emit structured logs, metrics and trace events to an observability layer which is governed by NeHA based on open standards (e.g. OpenTelemetry, Prometheus). This enables end-to-end monitoring, auditing and performance tracking.

System Event Bus	An internal event distribution mechanism (based on publish-subscribe architecture) used to propagate state changes such as session initiation, accreditation submission and audit-relevant activity across modules. The event bus follows a publish-subscribe architecture and is compatible with message broker platforms such as Apache Kafka/ActiveMQ/RabbitMQ, enabling asynchronous workflows and loose coupling between modules.
Modular Data Persistence Cluster	A centrally provisioned relational database infrastructure supporting structured data persistence for all CY-EHDS-2nd functional modules (WP5–WP9). The cluster is deployed on the National Cloud Hosting Platform and is governed by NeHA, which enforces security, backup, and retention policies. CPL and observability components do not interact directly with this layer.
API Specification Registry	A governance service ensuring that all inter-module and public APIs follow versioned OpenAPI 3.0 schemas. Managed by NeHA, this registry enforces interface stability, semantic consistency and documentation alignment across CPL, DAAMs and nHDsC. The registry includes internal API specifications across CPL, DAAMs and nHDsC. Should any external interfaces be exposed (e.g. public metadata browsing), they will follow version-controlled OpenAPI 3.0 definitions and undergo governance review by NeHA.
CY Login (electronic Identification (eID))	The national authentication gateway through which all users authenticate. Integrated with CPL using OpenID Connect protocols, it ensures compliance with electronic ID, Authentication and Trust Services (eIDAS) and national digital identity policies.

Finally, in alignment with national requirements, the CY-EHDS-2nd infrastructure will support multilingual delivery in the official languages of the Republic of Cyprus (Greek and Turkish) and English. While the current deliverable and interface implementation are in English, all user-facing modules (e.g. CPL portals, metadata views) will incorporate internationalisation support. This includes locale-aware rendering of UI text, support for dual-language string resources and integration of translation workflows within the User Interface (UI) layers. Multilingual readiness will be implemented at front-end level, without altering business logic or shared API interfaces.

A.2.3.3 Logical Module Interactions

This section provides an overview of the logical interactions among the core modules of CY-EHDS-2nd. It focuses primarily on CPL-centric workflows while also listing other critical inter-module connections to illustrate the full system coordination. Detailed business logic, data flows and workflow mechanics are described in the respective WP deliverables (WP5–WP9). This section is meant to provide an overall systems view for context and architectural completeness.

Key orchestration patterns and module interactions include:

- **CPL – DAAMs**: CPL enforces session validity, role and accreditation before DAAMs APIs are exposed. Data access and request applications' submission and data permit lifecycle tracking are handled entirely within DAAMs.
- **CPL – nHDsC**: CPL authenticates and authorises Data Holders, enabling them to access the metadata management interfaces provided by nHDsC. All metadata presentation, retrieval and management logic are handled entirely by WP6. CPL does not retrieve or display metadata directly.
- **CPL – SPEs**: CPL authenticates and routes SPE Operator sessions to the Internal or External Secure Processing Environment (ESPE) based on role. CPL enforces identity verification, certificate validation and access control before entry. No dataset access occurs in CPL.

- **nHDsC – DQET**: WP9 provides data quality and utility labels on metadata records registered in nHDsC. These labels are associated with the respective records and displayed within nHDsC interfaces. CPL is not involved in labelling logic or delivery.
- **nHDsC – DAAMs**: When a data user builds an access application, the DAAMs receives the relevant Metadata Record ID from the nHDsC. This ensures precise dataset referencing and linkage between permit requests and registered data assets.
- **DAAMs – SPE**: Once a data permit or data request is granted, DAAMs forwards the project execution parameters to the Internal SPE. The Internal SPE queries and prepares the dataset, which is then securely transferred to the ESPE for delivery to the permitted data user. CPL does not participate in this interaction.
- **DAAMs & nHDsC–WP8 (NCP)**: For cross-border data permit, data request and dataset metadata records exchanges, both DAAMs and nHDsC provide the required structured data to the NCP. The NCP interfaces with the EU HealthData@EU infrastructure using the HealthData@EU Node specifications and eDelivery protocols.
- **Observability**: All modules, including CPL, DAAMs and nHDsC, emit logs, metrics and trace events into the shared observability infrastructure operated by NeHA. This enables unified monitoring, alerting and system auditability.

All user sessions, accreditation checks and access routing are initiated through CPL, which acts as the single-entry point for data users, data holders and HDAB authorised personnel.

A.2.3.4 Hosting and Observability Infrastructure

All modules are deployed on a shared, containerised national platform operated under the governance of NeHA. Each service runs in an isolated namespace with defined Continuous Integration/Continuous Deployment (CI/CD) pipelines managed centrally. NeHA also governs:

- API schema versioning (OpenAPI 3.0)
- Deployment approvals
- Configuration management
- Infrastructure access controls

Observability infrastructure is shared across all modules. Each emits logs, metrics and traces using a structured format and correlation ID schema. The infrastructure is compatible with OpenTelemetry and allows unified dashboards, alerts and historical audits. All observability components are hosted within the national eHealth cloud, under NeHA operational responsibility.

A.2.4 Alignment with HealthData@EU CP

The architecture is closely aligned with the HealthData@EU CP reference model which serves as the basis for component interaction, APIs, security design and cross-border operations. The alignment ensures the following:

- Structural compatibility with central services, such as dataset search and permit synchronisation
- Use of common message formats (e.g. JavaScript Object Notation for Linked Data (JSON-LD), eXtensible Markup Language (XML)), catalogue schema and metadata vocabularies
- Adoption of open-source modules published by the EC
- Support for cross-border workflows via the national Dispatcher and Domibus gateway

The architecture reuses open-source components published by the Commission (where applicable) tailored to Cyprus legal and operational environment ensuring forward compatibility with future HealthData@EU CP

central upgrades. A high-level mapping of CY-EHDS-2nd components to the HealthData@EU Node reference architecture is provided in ANNEX C.

A.2.5 Modular and Scalable Design

Each CY-EHDS-2nd module is designed to be independently deployable and modular, enabling lifecycle separation between components such as DAAMs, the nHDsC and the SPE. Interfaces between CY-EHDS-2nd modules are designed according to the principle of loose coupling, as defined in the HealthData@EU CP architecture so that each module exposes well-defined APIs, enabling communication without requiring internal knowledge of other components.

Where applicable, modules are designed to be stateless, supporting scalability and flexible deployment options. All modules communicate via secure, standardised APIs that use message formats defined by the HealthData@EU CP specifications, including Health DCAT-AP for dataset descriptions andSHACL for metadata validation. Authentication and authorisation are managed through Cyprus national identity infrastructure, specifically via CY Login, in alignment with eIDAS principles.

API contracts and technical conformance will be validated using test scenarios and artefacts derived from the HealthData@EU CP Testing Framework [18]. Cross-module processes, such as the transition from application submission to permit issuance, will be supported via standardised APIs.

A.2.6 Stakeholders

The stakeholders with potential interest in CY-EHDS-2nd infrastructure are:

- The HDAB of Cyprus, NeHA which is the Business Owner and Solution Provider of this infrastructure.
- The EC Directorate General for Health and Food Safety (DG-SANTE) as the Business Owner and the Solution Provider of the HealthData@EU CP infrastructure.
- Data users, who are natural or legal persons having lawful access to personal or no-personal electronic health data for secondary use.
- Data holders, who are legal persons, governmental bodies, primary use and secondary use organisations having lawful right to create, collect and store personal data or no-personal electronic health data for primary or secondary use.
- Health-related research infrastructures or similar structures, whose functioning is based on Union and national law and which support the use of electronic health data for research, policy makings, statistical, patient safety or regulatory purposes.

A.2.7 Actors

The actors of the CY-EHDS-2nd platform are divided into two categories, human actors and system actors and are outlined in *Annex D: Common Actor Definitions – CY-EHDS-2nd (v1.0)* while Table A. 7 and Table A. 8 present the actions allowed per actor.

[18] SC022_D03.03_Testing Framework_Scale-Up_SANTE APPROVED

Table A. 7: Human Actors of the CY-EHDS-2nd

Actor	Authentication	Access and search for Dataset Catalogues, and their relevant records	Manage Application Lifecycle (create, update, submit, delete)	Manage Data Permit Lifecycle (create, amend, revoke)	Application Evaluation / Internal Comments	Access and use SPE	Configure SPE	Access and use internal SPE	Review data quality and utility labels	Review dataset descriptions	Submit Metadata Records	CRUD on Catalogue	Reporting / KPIs	Administration Capabilities (e.g. User Management)
General Public Citizen		TRUE												
Data User	TRUE	TRUE	TRUE			TRUE								
Data Holder	TRUE	TRUE									TRUE			
HDAB Application Manager (NeHA)	TRUE	TRUE	TRUE											
HDAB Data Permit Manager (NeHA)	TRUE	TRUE		TRUE										
Application Reviewer	TRUE	TRUE			TRUE									

/Evaluator													
nHDsC Manager (NeHA)	TRUE	TRUE									TRUE		
nHDsC Auditor (NeHA)	TRUE	TRUE							TRUE				
DQET Manager (NeHA)	TRUE	TRUE						TRUE					
Internal SPE Operator (NeHA)	TRUE	TRUE				TRUE	TRUE	TRUE					
SPE Operator (NeHA)	TRUE	TRUE				TRUE	TRUE						
HDAB Business Owner / Solution Provider	TRUE	TRUE										TRUE	
System Administrator	TRUE	TRUE										TRUE	TRUE

Table A. 8: System Actors of the CY-EHDS-2nd

Actor	Sync Dataset Metadata	Sync App Status	Sync Permit	Send Cross-Border App/Permit
HealthData@EU CP (System Actor)	TRUE	TRUE	TRUE	TRUE

A.2.8 Component Architecture

The CY-EHDS-2nd architecture is composed of five core functional modules and one horizontal enabling layer. Each module corresponds to a specific set of the HDAB DBCs blueprint and supports compliance with EHDS. These components interact through secure, standardised APIs and are designed for modular deployment, role-based access and cross-border interoperability.

The architecture includes a CY-EHDS-2nd CPL, which provides the shared services required to support secure, trusted and auditable operations across the entire system. This layer is not considered a standalone module, as it does not provide a business function in itself but serves as the technical and governance backbone of the platform. Each functional module runs independently but relies on the CPL for user authentication, access control and secure routing.

The overall CY-EHDS-2nd architecture is depicted in Figure A.3 and each of its components is comprehensively presented in the following sub-sections.

A.2.8.1 CY-EHDS-2nd CP Layer

The CY-EHDS-2nd CP Layer is the central access and orchestration layer that provides identity, session, role, accreditation and observability services to all user-facing workflows. These services are implemented as modular, reusable components referred to as CPL Shared Services (CPSS1–CPSS4), which are consumed by the other modules without duplication and are presented in Table A. 9. All services are deployed on the same national Kubernetes infrastructure managed by NeHA, except for the SPE, which is hosted in a logically isolated secure environment.

Table A. 9: CY-EHDS-2nd CP L shared services

Code	Service Name	Description	Dependent Modules
CPSS1	**Identity and Access Management**	Manages login via CY Login, session token creation and identity propagation.	All modules via CPL
CPSS2	**User Profile and Accreditation Services**	Displays profile info, manages accreditation submission and status.	DAMMs, nHDsC
CPSS3	**Role Management**	Enforces role selection at session start and applies RBAC across APIs.	All modules via CPL tokens
CPSS4	**Logging, Monitoring, and Audit**	Emits structured logs and security events to shared observability backend.	All modules

All CPSS components are governed by NeHA and exposed only through CPL. Other modules consume these services via secure internal APIs or shared tokens, without implementing parallel logic.

NeHA also governs the API versioning of all inter-module REST interfaces, ensuring alignment with OpenAPI 3.0 specifications. Any changes to schema definitions or interface behaviour are reviewed through a central governance process.

Accreditation workflows, including document uploads and approval steps, are presented through CPL front-end interface. However, all accreditation data is securely transferred to and stored by NeHA-controlled systems. CPL does not persist accreditation documents, in compliance with data minimisation and legal separation of responsibilities.

Requests to delete user accounts are initiated through CPL but executed by the Profile Service, which handles downstream deletion across DAAMs, nHDsC and related services. CPL itself does not remove identity records directly.

All CPL session tokens carry a session language attribute (e.g. lang=en, lang=el, lang=tr). This language value is respected by all user-facing modules (DAAMs, nHDsC, etc.), which render interface text and error messages in the corresponding language. If a translation is unavailable, the original content is displayed as a fallback.

A.2.8.2 Data Access Application Management solution (DAAMs – WP5)

The DAAMs is a core functional module of the CY-EHDS-2nd infrastructure. It provides the end-to-end workflow for managing data access applications, from submission by accredited users to the final issuance or rejection of permits by NeHA (HDAB). DAAMs operates in full compliance with the EHDS regulation and thus, it interfaces with the HealthData@EU infrastructure besides the national secondary use of health data infrastructure.

DAAMs builds on top of the CP Layer relying on the shared services for user authentication (via CY Login), role enforcement, accreditation and secure user interaction.

This module is covered in detail in its dedicated deliverable: D5.1 - DAAMs Requirements, Specifications and Prototype, which outlines its functional design and implementation requirements including:

- Application submission
- Application lifecycle management
- Permit workflow

A.2.8.3 National Health Dataset Catalogue (nHDsC – WP6)

The nHDsC is a key functional module of the CY-EHDS-2nd infrastructure. It serves as the central metadata registry for health datasets available for secondary use within the Republic of Cyprus jurisdiction. The nHDsC enables discoverability, transparency and alignment with the requirements of Article 60 of the EHDS regulation while ensuring technical and semantic interoperability with the HealthData@EU CP catalogue.

nHDsC also builds on top of the CP Layer leveraging the shared services such as user authentication, role-based permissions and accreditation status. It also interfaces with the NCP to synchronise relevant metadata records with the HealthData@EU catalogue infrastructure.

This module is covered in detail in its dedicated deliverable “D6.1 - nHDsC: Requirements and Specifications” which thoroughly outlines its functional design and implementation requirements including:

- Metadata creation
- Metadata submission
- nHDsC management
- Dataset Discovery

A.2.8.4 Secure Processing Environment (SPE – WP7)

The SPE is a critical component of the CY-EHDS-2nd infrastructure that enables authorised data users to process health datasets under strict technical, legal and organisational controls. Its primary objective is to

ensure that data processing occurs in a secure, auditable and non-downloadable manner, in line with the requirements of the EHDS regulation and GDPR.

The CY-EHDS-2nd architecture foresees two distinct types of SPEs, both operated by NeHA (HDAB):

(A) Internal SPE: Used by NeHA to transform or prepare raw health data received from data holders, in accordance with the access permit and prior to delivery to the permitted data user.
(B) ESPE: Used by the permitted data user(s) to securely analyse datasets, without being able to download or export the data and only for the purposes defined in the approved data permit.

While both SPE components are designed as isolated environments with their own security perimeter and processing logic, they are interlinked with the DAAMs module, which governs the lifecycle and the conditions of permit issuance (e.g. what data may be accessed, by whom, for how long and under what constraints).

SPE environments do not implement or rely on business logic from the CY-EHDS-2nd CPL for processing or analytics. However, CPL does provide critical shared services required for secure access to the SPE by designated NeHA operators. Specifically, SPE operators (both Internal and External) must authenticate via the CPL using CY Login credentials and a browser-based client certificate. CPL validates both identity and certificate attributes at the ingress level before issuing a role-bound session token and routing access to the appropriate SPE instance ensuring centralised access enforcement, consistent audit logging and full traceability across the infrastructure.

All analytical functions, data transformations and user interactions with datasets occur strictly within the SPE environments, in accordance with technical and legal safeguards. The CPL is not involved in any data handling or execution logic beyond session validation and routing.

This module is covered in detail in its dedicated deliverable: “D7.1 – SPE: Requirements and Specifications,” which outlines its functional design and implementation requirements, including:

- Internal processing of raw health data
- Provisioning and access control for permitted data users
- Secure access and analysis of permitted datasets
- Audit, logging, and traceability of all operations within the SPE

A.2.8.5 National Connector for Cross-Border Gateway (WP8)

The National Connector for Cross-Border Gateway module is responsible for enabling the secure and standards-based exchange of secondary-use health data information between the CY-EHDS-2nd infrastructure and the HealthData@EU CP. This includes the transmission of health dataset metadata, application status updates and data permit/data request decisions to other Member States, as well as the reception of cross-border requests addressed to Cyprus.

This module comprises two sub-components:

(A) The National HealthData@EU Dispatcher, which handles orchestration, packaging, status management and logging of outgoing and incoming messages.
(B) The Cross-Border Gateway, a Domibus-based interface that ensures secure, traceable eDelivery of structured messages in accordance with the specifications of the HealthData@EU infrastructure.

The National Dispatcher is a component managed by CY-EHDS-2nd that integrates with internal modules (DAAMs, nHDsC) and the logging framework of the CP Layer. The Cross-Border Gateway is built on the Domibus eDelivery standard, as required by the HealthData@EU technical specifications. The Contact Point,

as defined in the architecture, acts as the logical interface between national systems and the EU CP and is operated as part of this module.

This module is covered in detail in its dedicated deliverable "D8.1 - National Connector for Cross-border gateway Requirements and Specifications" which thoroughly outlines its functional design and implementation requirements including:

- Metadata synchronisation
- Cross-border application reception
- Message validation and logging
- Inbound request handling

A.2.8.6 Dataset Quality Enhancement Toolbox (DQET – WP9)

The DQET is a dedicated module of the CY-EHDS-2nd infrastructure designed to support the assessment, annotation and improvement of the quality and utility of datasets made available for secondary use. The DQET ensures that datasets included in the nHDsC meet defined technical and semantic standards and it supports the transparent communication of quality information of data users, in alignment with the goals of the EHDS and HealthData@EU.

The toolbox will be developed in accordance with the EHDS regulation and aligned with the QUANTUM framework, which is being developed at EU level to provide a harmonised model for describing dataset fitness for secondary use.

DQET integrates with the nHDsC module, enriching metadata records with quality annotations before or after publication. DQET outputs are compatible with semantic validation frameworks (e.g. SHACL) and support extensibility for new EU-wide quality rules, as foreseen in future TEHDAS2 guidelines and EHDS implementing acts.

This module is covered in detail in its dedicated deliverable "D9.1 - Health data quality enhancement toolbox: Requirements and Specifications" which thoroughly outlines its functional design and implementation requirements including:

- Structured label management
- Data quality and utility label governance and validation framework

A.2.9 System Interactions and Workflow Overview

A high-level presentation of the runtime interactions between the core functional modules of CY-EHDS-2nd infrastructure and the principal actors involved is presented in Figure A. 3. It depicts how authenticated users interact with the platform through the CPL and how specific operations (e.g. dataset description publication, application submission, data quality enhancement, permit issuance and SPE access) are distributed across the system. The diagram also depicts how the CY-EHDS-2nd infrastructure connects with the HealthData@EU infrastructure via the WP8 Cross-Border Gateway, using structured metadata and permit exchange mechanisms governed by the NPC. The interaction flow visualised in this figure supports both national and cross-border use cases (UCs) and clarifies the role of each component and actor within the CY-EHDS-2nd ecosystem.

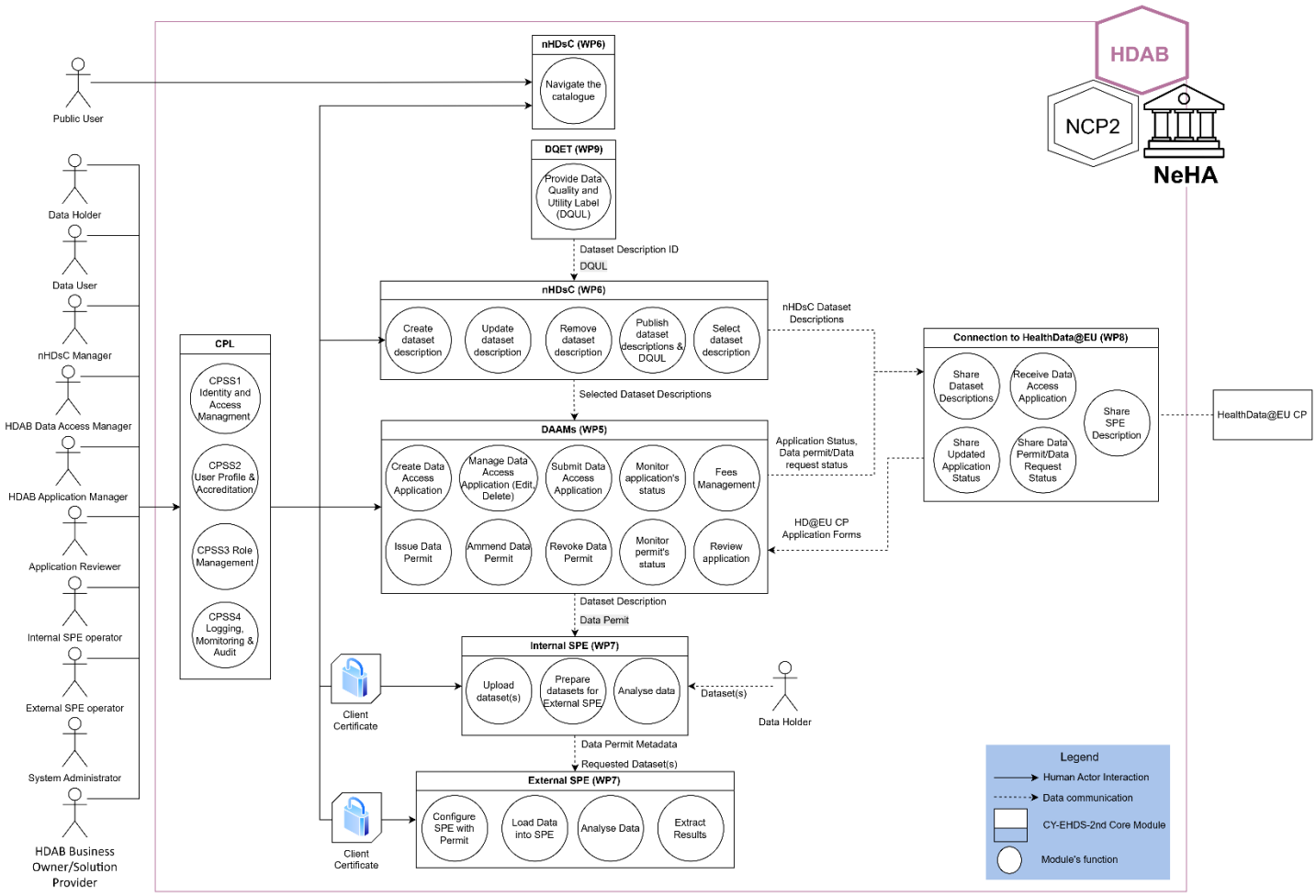

Figure A. 3: Logical Interactions Across CY-EHDS-2nd Core Modules

A.2.10 CY-EHDS-2nd Technical Architecture

The layered architecture of the CY-EHDS-2nd infrastructure, including its five core functional modules (WP5–WP9), the CPL with its shared services (CPSS1–4), cross-cutting technical components (e.g. observability stack, configuration management, CI/CD pipeline, localisation service) and external integration points (e.g. CY Login, HealthData@EU CP) is depicted in Figure A. 4 It reflects the modular deployment of the infrastructure on a shared national Kubernetes platform and highlights key dependencies such as API gateways, the event bus, shared observability infrastructure and multilingual support services and shared data persistence services. It also illustrates how user sessions, authentication, accreditation and inter-module orchestration are handled centrally by the CPL and how logs, metrics, and asynchronous system interactions are propagated through the shared observability stack and event bus infrastructure. NeHA, acting both as the HDAB and NCP, governs the infrastructure in alignment with EHDS and HealthData@EU specifications.

The architecture is logically organised into three horizontal layers plus a national hosting substrate that underpins the infrastructure:

1. **Functional Module Layer (Green Layer)**
   This layer hosts the five core functional modules developed under WPs 5–9:
   - **DAAMs (WP5)**: Supports application submission, permit lifecycle and HDAB decision tracking.
   - **nHDsC (WP6)**: Manages dataset descriptions (metadata records) registration, validation, discovery and alignment with Health DCAT-AP standard.

- **SPE (WP7)**: Composed of Internal SPE (data preparation) and ESPE (user analysis). Permitted access only.
- **DQET (WP9)**: Supports creation of dataset quality and utility labels, consumed by nHDsC.
- **Cross-border Connection (WP8)**: Includes the National Dispatcher, Cross-Border Gateway (Domibus) and NCP for communication with the HealthData@EU CP.

Each module connects to shared services for access control, logging and session context. All interactions with users and external actors are authenticated and authorised centrally via CPL.

2. **Cross-Cutting Infrastructure Layer (Blue Layer)**
   This layer represents shared technical services that are reused across all functional modules. These services are operated centrally by NeHA and include:
   a. **CPL**: Manages identity, session control, role enforcement and accreditation routing. Acts as the access gateway to all internal services. CPL Shared Services (CPSS1–CPSS4):
      i. CPSS1: Identity and Access
      ii. CPSS2: Profile and Accreditation
      iii. CPSS3: Role Management
      iv. CPSS4: Audit Logging and Monitoring
   b. **Shared Relational Database Cluster:** Provides persistent storage for all module-level data (e.g. applications, metadata, quality labels), implemented as a secure, centralised database cluster serving the DAAMs, nHDsC, DQET, and other components. Each module uses dedicated schemas or logical partitions to maintain data separation and enforce access control. Audit and logging data are excluded and handled by the observability stack.
   c. **Shared Observability Stack**: Aggregates logs, metrics and traces from all modules (DAAMs, nHDsC, SPE, etc.) into a central monitoring layer.
   d. **Event Bus**: Enables asynchronous communication between modules using event-driven architecture (e.g. ApplicationSubmitted, QualityLabelCreated).
   e. **CI/CD Pipeline**: Automates deployment and testing workflows.
   f. **Secrets & Configuration Management**: Ensures consistent and secure configuration across all containers.
   g. **Profile Service**: Manages account lifecycle events, including GDPR-aligned deletion.
   h. **Language Localisation Service**: Provides translation and fallback support for multilingual UIs (English, Greek, Turkish).
   i. **API Gateway / Ingress Controller**: Routes secure inbound traffic to CPL services.

   This layer is cross-cutting, supporting both system orchestration and lifecycle management. It ensures traceability, auditability, and governance enforcement across all operational services.
3. **Identity, Entry Points, and External Systems Layer (Orange Layer)**
   This layer includes all external and identity-facing components and their integration points:
   - **CY Login**: The national electronic identity federation gateway, accessed via OIDC. All users (data holders, users, SPE officers, NeHA officers, revirewers, etc.) must authenticate here.
   - **HealthData@EU CP**: EU-level infrastructure interfacing via WP8. Exchanges dataset descriptions and data permit/request forms and decisions using AS4/eDelivery.

   This layer connects the CY-EHDS-2nd infrastructure to both external actors (e.g. HealthData@EU CP) and national services (e.g. identity, hosting), ensuring secure and legally compliant integration.
4. **National Cloud Hosting Platform (yellow rectangle):** The Cross-Cutting Layer and Functional Modules Layer are architecturally and operationally hosted within the National Cloud Hosting Platform. All its components are deployed as containerised microservices in a shared Kubernetes cluster, with each WP operating in its own namespace. This platform is fully operated and governed

by NeHA in its role as the HDAB, ensuring regulatory compliance, service reliability, and operational isolation where required. The NCP (WP8) is also hosted within this platform.

The Identity, Entry Points and External Systems Layer, however, includes external actors and systems and is not part of the national cloud infrastructure. It is accessed via secure, standardised protocols (e.g. OpenID Connect , eDelivery) through designated ingress and communication components governed by CPL and WP8.

A.3 CY-EHDS-2ND CENTRAL PLATFORM LAYER REQUIREMENTS AND SPECIFICATIONS

The CPL of the CY-EHDS-2nd infrastructure provides the essential cross-cutting services required to enable secure and interoperable secondary use of health data in Cyprus. It acts as the foundational layer supporting all functional modules, including the DAAMs, the nHDsC, the SPE, the National Connector and Cross-Border Gateway and the DQET.

The CPL delivers critical services such as user authentication through CY Login, role-based access control, user accreditation workflows, technical audit logging, system monitoring and the orchestration of cross-border messaging with the HealthData@EU infrastructure. It ensures consistent enforcement of security, legal and governance requirements across the CY-EHDS-2nd ecosystem, while promoting modularity, scalability and legal compliance.

The technical and functional specifications of the CPL are designed to fully align with the EHDS regulation, GDPR principles and the technical guidelines set out by the HealthData@EU CP specifications. By centralising these shared capabilities, the CPL enables efficient integration across modules while minimising duplication, ensuring that national infrastructure of the secondary use of health data of Cyprus remains secure, future-proof and interoperable.

A.3.1 Functional Requirements

This section defines the functional requirements for the CY-EHDS-2nd CPL. The requirements are organised according to the shared services domains (CPSS1–CPSS4) that the CPL provides across the national secondary use infrastructure. The specific functionalities that the CPL must deliver in order to support secure, lawful and interoperable operations, in alignment with the EHDS Regulation, GDPR and the HealthData@EU infrastructure are provided per each shared service domain in Table A. 10.

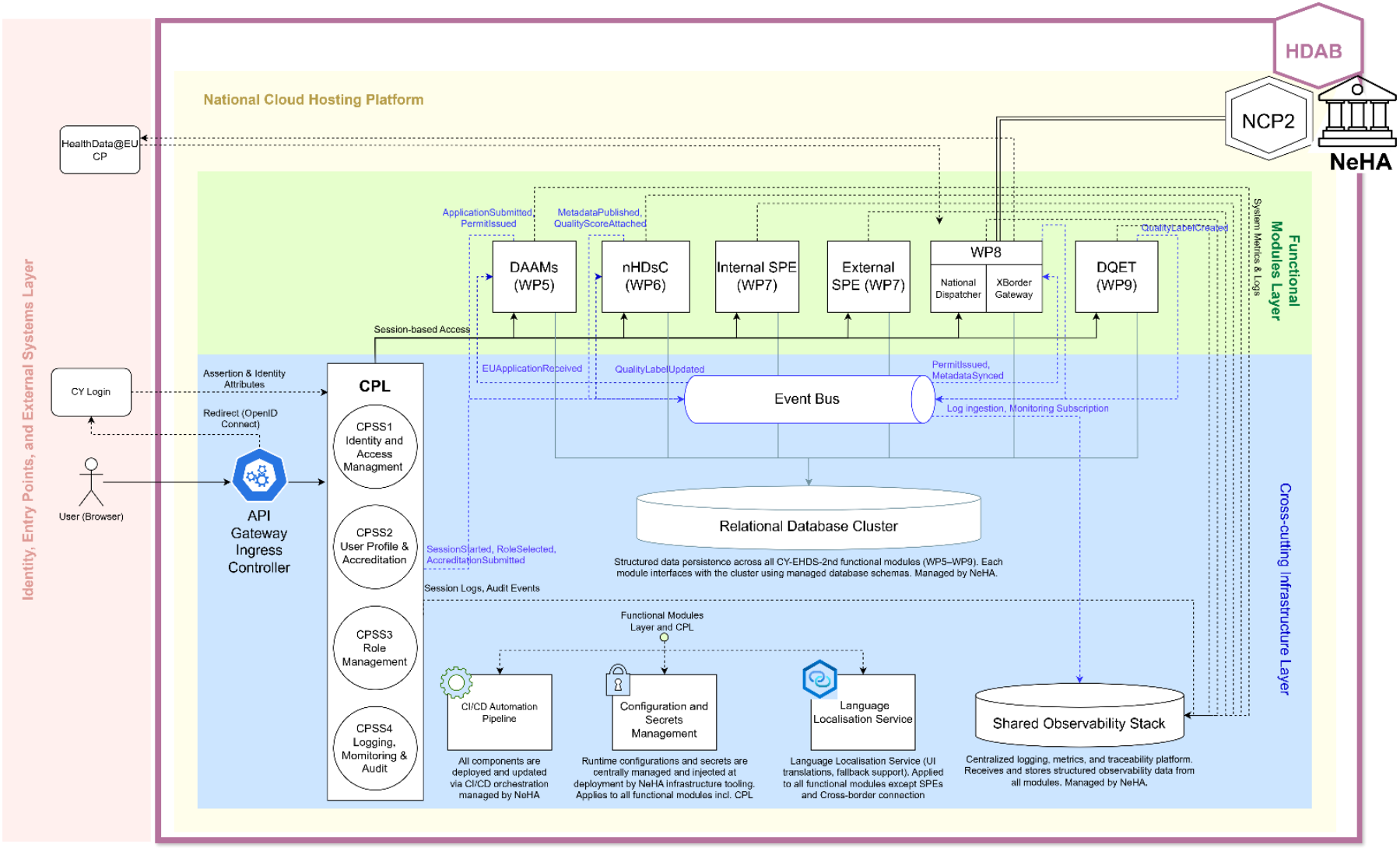

Figure A. 4: CY-EHDS-2nd Technical Architecture Overview

Table A. 10: CY-EHDS-2nd Functional Requirements per CPSS

CPSS Reference	CPSS1 – Identity and Access Management
Requirement Code	**CPL-FR1**
Requirement Title	User Authentication
Involved Actors	Data User (Natural/Legal), Data Holder, HDAB Application Manager, HDAB Data Permit Manager, nHDsC Manager, HDAB Business Owner, System Administrator
Requirement Features	- Authenticate users via CY Login
	- Retrieve immutable identity attributes
Detailed Description	The CY-EHDS-2nd CPL must authenticate all users through the national CY Login service. Upon successful authentication, the CPL must retrieve and store the user's immutable identity attributes, including name, surname, type (natural/legal) and affiliated organisation. No internal credential management is permitted. The CPL must enforce secure session management practices, including mandatory session timeouts and forced re-authentication after periods of inactivity. For access to SPEs, designated NeHA operators must also present a valid client certificate issued by NeHA. The CPL must validate this certificate at the ingress level before allowing access to SPE-specific routes or issuing the SPE Operator session role. Both CY Login authentication and certificate validation must succeed for SPE access to be granted.
UCs	CPL-UC 1: CY Login Authentication A user accesses the CY-EHDS-2nd CPL portal. The system redirects them to CY Login for authentication. After successful login, identity attributes (name, legal/natural type, organisation) are retrieved and stored for session use.
	CPL-UC2: Failed Authentication Attempt A user fails to authenticate via CY Login (e.g. invalid credentials or revoked account). The system blocks access and logs the failed attempt for audit.
Requirement Code	**CPL-FR2**
Requirement Title	Session Role Selection after Authentication
Involved Actors	Data User (Natural/Legal), Data Holder, HDAB Application Manager, HDAB Data Permit Manager, nHDsC Manager, HDAB Business Owner
Requirement Features	- Allow users to select an active role after authentication
	- Enforce role-specific session permissions based on selected role
	- Support role assignment for natural persons with no organisational affiliation
	- Validate organisational accreditation if required
Detailed Description	After successful authentication via CY Login, users must be prompted to select a single active session role from among those assigned to them. This role governs all access rights and available actions during the session. The CPL must derive available roles from the user's identity attributes and accreditation status, including: • Organisation-linked roles (e.g. Data Holder) requiring prior accreditation, and • Individual-level roles (e.g. Natural Person - Data User) available without accreditation. The CPL must enforce RBAC uniformly across routed services based on this selection. This FR addresses runtime session behaviour, while system-wide role definition and assignment are governed under CPL-FR9.

UCs	CPL-UC3: Role Assignment Based on Accreditation After login, the CPL checks the user's accreditation record. If accredited, one or more roles (e.g. Data Holder, Data User) are assigned for session selection. If the user operates as a natural person not representing a legal entity, a role may be assigned without accreditation.
	CPL-UC4: Role Selection at Login A user who holds multiple roles (e.g. Catalogue Manager and Data Holder) is prompted to select one role before proceeding to access the system. The selected role governs access permissions for that session.
Requirement Code	**CPL-FR3**
Requirement Title	Public Access to CY-EHDS-2nd Components
Involved Actors	General Public (Anonymous User)
Requirement Features	- Allow unauthenticated access to public dataset catalogue metadata
	- Allow unauthenticated access to fee structure and pricing methodology
	- Allow unauthenticated access to static content on applications' related information
	- Restrict unauthenticated users to read-only actions
	- Prevent access to any submission or modification features
Detailed Description	The CY-EHDS-2nd CPL must allow members of the public to access certain informational components of the platform including: 1. Browse and search metadata records in the nHDsC without requiring authentication via CY Login. Public users must be granted only read-only access to public metadata fields and must not be able to submit, modify, annotate, or otherwise interact with any dataset records. 2. Static explanatory content under the DAAMs section covering information related to DAAMs operations and functionalitites 3. A view of the official fee model and pricing structure for data access or request applications. All functions requiring authentication, accreditation, or submission rights must be hidden or disabled for unauthenticated users.
UCs	CPL-UC5: Public Search of Dataset Catalogue A public user (not logged in) accesses the nHDsC. They are allowed to search and view published metadata records.
	CPL-UC6: Restricted Action by Anonymous User A non-authenticated visitor tries to perform a restricted action (e.g. submit metadata or application). The system redirects the user to the CY Login authentication flow.
	CPL-UC20: Read Public Application and Fee Information An anonymous visitor accesses the DAAMs section to read about the application process and view the fee structure without login.
CPSS Reference	**CPSS2 – User Profile and Accreditation Services**
Requirement Code	**CPL-FR4**
Requirement Title	User Profile Dashboard
Involved Actors	Data User (Natural/Legal), Data Holder
Requirement Features	- Display immutable identity information
	- Display accreditation status and linked organisations
	- Display account management options

Detailed Description	The CY-EHDS-2nd CPL must provide each authenticated user with a dashboard summarising their immutable identity attributes retrieved from CY Login, their accreditation status and their accredited organisations, if any. The dashboard must offer clear access to self-service account management options, including account deletion (where applicable). Users must not be able to modify their verified identity information from within the CPL.
UCs	CPL-UC7: Accessing User Profile Dashboard An authenticated user opens the profile dashboard to view their verified identity attributes, accreditation status and account settings. The dashboard content dynamically reflects the user's current session role (e.g. showing organisational affiliation only if acting as an accredited representative).
Requirement Code	**CPL-FR5**
Requirement Title	Accreditation Verification and Enforcement
Involved Actors	Data User (Natural/Legal), Data Holder, HDAB Accreditation Officer (back-office actor, indirectly)
Requirement Features	- Check accreditation status after role selection
	- Deny access to role-restricted functions if accreditation is missing
	- Link user to accredited organisation (if applicable)
Detailed Description	The CY-EHDS-2nd CPL must verify the accreditation status of users where applicable. Accreditation is required only for users who declare they are acting on behalf of a legal entity, organisation, or public body. In these cases, the CPL enforces a rule that users may not access controlled functionalities (e.g. submitting data access applications or publishing dataset metadata) until accreditation has been completed and approved. Users acting solely as natural persons (acting in a personal capacity) may access permitted features without accreditation, in accordance with their assigned role.
UCs	CPL-UC8: Block Access Pending Accreditation A user who claims to act on behalf of an organisation but has not completed accreditation is blocked from accessing the data access application submission interface until accreditation is granted.
	CPL-UC9: Bypass Accreditation for Independent User A user not representing any legal entity (i.e. acting in a personal capacity) is allowed to access catalogue and permitted functionality without accreditation being required.
Requirement Code	**CPL-FR6**
Requirement Title	Accreditation Request Submission
Involved Actors	Data User (Natural/Legal), Data Holder
Requirement Features	- Provide an online form for accreditation requests
	- Allow upload of supporting documentation
	- Capture intended organisation affiliation and role type
	- Track accreditation request status

Detailed Description	The CY-EHDS-2nd CPL must allow authenticated users to submit a manual accreditation request through their user dashboard. The request must capture information including the user's intended organisation affiliation, intended role (e.g. Data Holder, Data User) and supporting documentation required for verification (such as proof of employment, mandate letters, or institutional authorisations). The CPL must allow users to track the status of their accreditation request (e.g. pending, approved, rejected). Submission must trigger a workflow accessible by authorised NeHA officers for review.
UCs	CPL-UC10: Submitting an Accreditation Request A user logs in and submits an accreditation request, providing documentation linking them to a legal entity. The request is stored and routed to NeHA for review.
Requirement Code	**CPL-FR7**
Requirement Title	Accreditation Decision Management by NeHA
Involved Actors	HDAB Business Owner / Solution Provider (NeHA Back-office Actor)
Requirement Features	- Review accreditation requests and supporting documents
	- Approve or reject accreditation requests
	- Record accreditation decision and justification
	- Notify user of accreditation outcome
Detailed Description	The CY-EHDS-2nd CPL must allow authorised NeHA accreditation officers to review submitted accreditation requests and their supporting documentation through a secure administrative interface. Officers must be able to approve or reject each accreditation request, record the decision (including optional justification notes) and trigger a status update visible to the user. Upon approval, the user must be officially linked to the accredited organisation and role. The system must automatically notify the user of the accreditation outcome (approval or rejection). Accreditation decisions must be logged for auditability and traceability.
UCs	CPL-UC11: Approving an Accreditation Request A NeHA officer reviews the submitted documentation and approves the accreditation request. The user's profile is updated to reflect the linked organisation and role permissions are unlocked.
	CPL-UC12: Rejecting an Accreditation Request The NeHA officer rejects the request due to incomplete or unverifiable documentation. The user is notified and prompted to reapply.
Requirement Code	**CPL-FR8**
Requirement Title	User-Initiated Account Deletion
Involved Actors	Data User (Natural/Legal), Data Holder
Requirement Features	- Provide a self-service option to request account deletion
	- Trigger account deactivation and data removal procedures
	- Ensure deletion in compliance with GDPR and applicable retention policies

Detailed Description	The CY-EHDS-2nd CPL must provide authenticated users with a secure self-service option to request the deletion of their user account. Upon submission of a deletion request, the system must deactivate the user's account, remove associated profile information and record the deletion event in an audit log. Account deletion must comply with GDPR requirements regarding user rights to erasure and data retention periods. Any obligations for minimum data retention (e.g. retention of audit trails for security purposes) must be respected as per applicable law. Users must be informed about the effects of account deletion before confirming the action.
UCs	CPL-UC13: Account deletion A user accesses the profile dashboard and selects the option to delete their account. The system requests confirmation, performs the deletion and issues a data deletion log entry according to retention policy.
CPSS Reference	**CPSS3 – Role Management**
Requirement Code	**CPL-FR9**
Requirement Title	Functional Role Definition and Assignment Governance
Involved Actors	Data User (Natural/Legal), Data Holder, HDAB Business Owner / Solution Provider
Requirement Features	- Maintain a centrally defined, version-controlled list of functional roles
	- Assign roles based on CY Login identity and accreditation status
	- Ensure immutability of role mappings during session execution
	- Persist assigned roles securely for audit, review, and revocation management
	- Enable session role selection in alignment with CPL-FR2
Detailed Description	The CY-EHDS-2nd platform must implement a centrally governed list of functional roles, including: Data User, Data Holder, HDAB Application Manager, HDAB Data Permit Manager, nHDsC Manager, and HDAB Business Owner. Each authenticated user is assigned one or more roles based on verified identity attributes and accreditation outcomes issued via CPSS2. Role assignment must be securely persisted, audit-traceable, and version-controlled. This functional requirement governs the definition, assignment, and system-wide governance of roles. Session-level role selection and enforcement are addressed in CPL-FR2 under CPSS1
UCs	CPL-UC14: Role Assignment Based on Accreditation A data user who has completed accreditation is automatically assigned the role “Data User” linked to their verified organisation.
	CPL-UC15: Role Catalogue Update by NeHA A NeHA-authorised platform administrator updates the list of recognised functional roles. The updated role list is propagated to CPSS1 and applied in future logins.
Requirement Code	**CPL-FR10**
Requirement Title	Role-Based Access Enforcement
Involved Actors	All authenticated users (role-dependent), System Services
Requirement Features	- Enforce access to platform functions based on user’s active role
	- Block access to functions not permitted for a user’s session role
	- Allow shared services to query and verify active user roles during each session
	- Ensure that modules like DAAMs, nHDsC and DQET respect role boundaries

Detailed Description	The CY-EHDS-2nd CPL must implement and enforce RBAC consistently across all components. Once a user logs in and selects a session role, the CPL must enforce restrictions ensuring that the user only sees and can access functionalities and workflows permitted for that role. Each request to CPL services or linked modules must be validated against the user's active role. For example, only users with the "HDAB Application Manager" role may triage or approve data access applications and only users with the "nHDsC Manager" role may perform Create Read Update and Delete (CRUD) actions on catalogue records. Access enforcement must apply both at the API and UI layers and must be traceable through audit logs. Role-based access decisions are dynamically enforced based on the currently active session role. All access rights are validated at runtime before forwarding requests to underlying modules.
UCs	CPL-UC16: Blocking Unauthorized Access Attempt A Data User attempts to access permit configuration tools in DAAMs but is blocked because their role lacks those permissions.
	CPL-UC17: Authorised Access to Catalogue Management Tools A user with the "nHDsC Manager" role is granted access to publish and manage metadata records in the national catalogue.
CPSS Reference	**CPSS4 – Logging, Monitoring and Audit**
Requirement Code	**CPL-FR11**
Requirement Title	Audit Logging of User and System Actions
Involved Actors	all authenticated users, HDAB Business Owner / Solution Provider, System Administrator, System Services
Requirement Features	- Record all platform-level actions, including logins, role switches and sensitive transactions - Maintain immutable, tamper-evident audit logs of all user and system actions. - Support session-based correlation IDs - Enable audit trail exports for authorised reviewers
Detailed Description	The CY-EHDS-2nd CPL must capture a detailed and immutable audit trail of key user and system actions. This includes login attempts, role selections, access to controlled interfaces, accreditation actions, account changes and interactions with DAAMs, nHDsC and other platform modules. Each log entry must include a timestamp, session ID, user identity and the nature of the action. The audit logs must be stored in a tamper-evident system, retained in accordance with legal data retention periods and accessible only to authorised roles for review or export.
Use Cases	CPL-UC18: Logging of Role-Specific Access Event A user acting under the "Data Holder" role accesses the metadata submission interface. The CPL logs the event with timestamp, user ID, session role and interface accessed.
	CPL-UC19: Retrieval of Audit Trail by Auditor A NeHA officer queries the CPL logging interface to retrieve a filtered audit trail of all data access application evaluations performed over a selected time window. Access to logs is granted only with audit-level role permissions.

A.3.2 Non-functional Requirements

This section defines the NFRs that govern the behaviour, performance and compliance attributes of the CY-EHDS-2nd CPL infrastructure. These requirements specify the system-wide qualities that the CPL must uphold to ensure operational robustness, legal compliance and alignment with European standards.

The NFRs have been structured in accordance with the international standard ISO/IEC/IEEE 29148:2018, which classifies system quality characteristics into distinct domains. This classification has been refined and adapted based on the specific roles of the CPL as a technical backbone for health data access, governance and cross-border interoperability under the EHDS regulation.

To ensure relevance, traceability and enforceability, the NFRs have been grouped under five main categories outlined in Table A. 11.

Table A. 11: Categories of the CY-EHDS-2nd CPL NFRs

No.	Category	Purpose
CNFRC1	Security & Access Control	Ensures the CPL enforces robust identity verification, role-based access, accreditation gating and auditability.
CNFRC2	Performance & Availability	Defines the system's ability to scale, remain available and respond within acceptable latency thresholds under normal and peak loads.
CNFRC3	Maintainability & Operability	Covers runtime configuration, monitoring and lifecycle support necessary for administrators and platform operators to manage the CPL securely and efficiently.
CNFRC4	Legal & Regulatory Compliance	Captures EHDS- and GDPR-driven obligations related to traceability, audit logs, retention, account management and rights of data subjects.
CNFRC5	Interoperability	Addresses semantic and technical compatibility with the HealthData@EU infrastructure, particularly in API specifications, metadata standards and security protocols.

Table A. 12 gives a thorough presentation of the CY-EHDS-2nd CPL NFRs. Each requirement is presented with a short description and a measure of compliance or testable indicator. It is important to note that these requirements apply exclusively to the CPL. NFRs for domain-specific modules are addressed in their respective WP deliverables.

Table A. 12: CY-EHDS-2nd CPL NFRs

Category	**CNFR1 - Security & Access Control**
Code	**CPL-NFR1**
Title	Secure Authentication Lifecycle
Description	The CPL must enforce strong authentication using the national CY Login service. All sessions must be securely initiated, scoped to the authenticated identity and terminated after defined periods of inactivity or token expiry. Session timeout and token lifetime policies shall be formally defined by NeHA.
	- Authentication uses CY Login with eIDAS-aligned protocol

Measure / Compliance Indicator	- Session and token expiration values are configurable and defined in NeHA security policy
	- Inactivity timeout and re-authentication rules enforced per policy
Code	**CPL-NFR2**
Title	Role-Based Access Control Enforcement
Description	The CPL must restrict all functionality access based on the user's active session role. Role definitions, permission mappings and scoping rules shall be centrally maintained by NeHA. Multi-role users must select one role per session. The CPL enforces access at runtime and roles are immutable throughout the session. All role information is retrieved from trusted identity or role registries. CPL does not create or modify user roles.
Measure / Compliance Indicator	- Role catalogue is centrally defined and enforced
	- Access control decisions enforced in UI and API layers
	- All modules (DAAMs, nHDsC, SPE) validate incoming tokens for role scope
	- NeHA maintains authoritative mapping of roles to permitted actions
	- Session role is immutable during the session lifecycle
Code	**CPL-NFR3**
Title	Accreditation Enforcement Prior to Action
Description	The CPL must ensure that platform actions requiring affiliation with a legal entity (e.g. metadata publication, data access application) are restricted to accredited users. Accreditation policies—including whether independent natural persons may act without affiliation—shall be formally defined by NeHA.
Measure / Compliance Indicator	- System gates critical actions based on accreditation flag
	- Accreditation enforcement applies before UI rendering and API calls
	- NeHA defines accreditation eligibility, documentation, and exceptions
	- Accreditation data is traceable and verifiable per session
Code	**CPL-NFR4**
Title	Tamper-Proof Logging and Traceability
Description	The CPL must maintain immutable logs of authentication, role selection, access attempts, configuration actions and permit-related events. Log retention periods shall be defined by NeHA. All logs must be traceable, pseudonymised where appropriate and auditable complied with EHDS regulation and GDPR. Logs must ensure cryptographic integrity using mechanisms such as append-only storage, hash chaining, or digital signatures.
Measure / Compliance Indicator	- Logging uses tamper-evident mechanisms (e.g. hash chaining or append-only storage)
	- Logs accessible only to authorised roles
	- Retention duration defined by NeHA in accordance with data protection law
	- Logs include timestamp, user session ID, and action trace
Category	

Code	**CPL-NFR5**
Title	Platform Uptime and Availability
Description	The CPL must remain available with minimal service interruptions to ensure continuity for national and cross-border operations. A baseline availability target shall be established by NeHA as part of the platform's service level objectives. Until formally adopted, a default monthly availability of 99.5% shall apply. Availability must be monitored in real time and downtime must be logged and auditable.
Measure / Compliance Indicator	- Uptime ≥ **99.5%** monthly, unless otherwise defined by NeHA
	- Maintenance windows are pre-scheduled and logged
	- Monitoring system is in place with real-time alerting for outage events
	- Uptime records are auditable on request
Code	**CPL-NFR6**
Title	Response Time for User-Facing Interactions
Description	The CPL must provide responsive performance for users interacting with key platform services such as login, dashboard access and role switching. While EHDS does not impose strict latency thresholds, a default 95th percentile response time of under 1000ms shall be applied to user-initiated interactions unless otherwise specified by NeHA. These thresholds must be actively monitored and may be adjusted based on observed platform behaviour.
Measure / Compliance Indicator	- 95th percentile latency: < **1200ms** for UI and API
	- Performance indicators tracked per session or role
	- Response Service Level Agreement (SLAs) apply during primary usage windows (e.g. 08:00–18:00 EET)
	- Thresholds adjustable under NeHA performance policy
Code	**CPL-NFR7**
Title	Scalability and Load Tolerance
Description	The CPL must sustain operational performance under normal and peak usage conditions, including concurrent user sessions and batch interactions. The system must degrade gracefully under pressure and, where technically supported, provide vertical or horizontal scaling. The CPL must support container-based deployment and horizontal scaling using orchestration technologies (e.g. Kubernetes). Target concurrency thresholds shall be validated by NeHA during production readiness testing.
Measure / Compliance Indicator	- Minimum support for 50 concurrent sessions under stress
	- Batch metadata actions (>50/min) do not degrade core services
	- Load testing results reviewed annually and thresholds updated if needed
	- CPL supports horizontal scaling using orchestration technologies (e.g. Kubernetes). Deployment manifests are version controlled.
Category	**CNFR3 -Maintainability & Operability**
Code	**CPL-NFR8**
Title	Administrative Runtime Configuration

Description	The CPL must allow authorised administrators to modify selected system-level configuration parameters (e.g. session timeout, logging level, service endpoint references) through a controlled and secure process. Where technically supported by the hosting architecture, such changes should be possible without full redeployment. All changes must be logged, versioned and access-controlled.
Measure / Compliance Indicator	- Only authorised roles (System Administrator or HDAB Business Owner) may apply configuration changes
	- Change history is retained with timestamp and user identity
	- Where supported, selected parameters are updateable without downtime
	- Configuration parameters are stored externally from application binaries
Code	**CPL-NFR9**
Title	Monitoring and System Health Visibility
Description	The CPL must implement internal monitoring for service uptime, authentication flows, role changes, accreditation actions and user-facing API availability. Monitoring must include key operational metrics such as endpoint health, request latency and error rates. For cross-border operations, the CPL may consume read-only event summaries (e.g. from WP8 logs) to provide NeHA operators with operational awareness, but it does not generate or own any eDelivery-level observability.
Measure / Compliance Indicator	- Internal service metrics collected via Prometheus or equivalent
	- CPL logs consumed into central NeHA observability dashboard
	- Role-based access to logs enforced
Code	**CPL-NFR10**
Title	Deployability and Configuration Consistency
Description	The CPL must support secure and consistent deployments through a repeatable mechanism. Where technically feasible and appropriate for the hosting stack, rollback to a previously known-good version should be supported. Configuration files must be externalised and managed through version control. This requirement is conditioned by the hosting and operational model adopted by NeHA.
Measure / Compliance Indicator	- Deployment scripts or orchestration tools support reproducible builds
	- Configuration is version-controlled and separated from executable code
	- Rollback support is documented and tested where technically feasible
Category	**CNFR4 -Legal & Regulatory Compliance**
Code	**CPL-NFR11**
Title	User-Initiated Account Deletion and Data Minimisation

Description	The CPL must support GDPR-compliant account deletion, allowing authenticated users to request the erasure of their account and associated personal data. Deletion must trigger account deactivation and data minimisation procedures. NeHA shall define which data elements must be retained to fulfil legal or security obligations.
Measure / Compliance Indicator	- Account deletion feature available via CPL dashboard
	- Deletion logs created and pseudonymised
	- Only legally required data (e.g. audit trails) retained
	- NeHA defines: deletion scope, mandatory retention elements and audit procedures
Code	**CPL-NFR12**
Title	Personal Data Access and Transparency
Description	The CPL must offer users a clear view of their identity attributes (retrieved from CY Login) and accreditation status through a secure profile dashboard. Correction of inaccurate data, if permitted, shall follow a process defined by NeHA.
Measure / Compliance Indicator	- User profile displays immutable identity data, active role and accreditation status
	- Read-only interface; updates handled outside CPL
	- NeHA defines which attributes are visible and how correction requests are handled
Code	**CPL-NFR13**
Title	Data Protection by Design and by Default
Description	CPL interfaces, workflows and APIs must enforce privacy-preserving defaults and prevent overexposure of personal data. Role scopes, session contexts and data payloads must reflect data minimisation principles. NeHA shall review and validate CPL privacy configurations at each major release.
Measure / Compliance Indicator	- CPL uses pseudonymisation and least-privilege data sharing
	- Attribute exposure is scoped to the active role and purpose
	- No unnecessary identifiers logged or displayed
	- NeHA approves privacy configurations and exception cases before production release
Code	**CPL-NFR14**
Title	Legal Record Retention and Evidence Preservation
Description	The CPL must retain its internal logs (authentication sessions, accreditation actions, role assignments, profile activity) according to national retention policies defined by NeHA. Retention settings must comply with GDPR and eIDAS traceability obligations.
Measure / Compliance Indicator	- Log retention policy defined by NeHA (e.g. 5 years for accreditation events)
	- Logs stored in tamper-resistant format
	- Secure deletion or archiving upon expiry
Category	**CNFR5 -Interoperability**
Code	**CPL-NFR15**
Title	National API and Protocol Conformance

Description	The CPL must expose and manage all APIs consumed by national modules (DAAMs, nHDsC, shared services), ensuring they conform to agreed technical standards. This includes RESTful patterns, OpenAPI 3.0 documentation, token-based access and internal consistency of identifiers. The CPL does not expose or mediate APIs to the EU CP or external Member States.
Measure / Compliance Indicator	- All internal CPL-facing APIs documented in OpenAPI 3.0
	- Role-based access tokens applied consistently
	- Interfaces versioned and governed by NeHA
	- Payloads align with internal schemas from DAAMs, nHDsC and CPSS

A.3.3 Technical Specifications

The CY-EHDS-2nd CPL is the national access and orchestration layer for authenticated interactions within the CY-EHDS-2nd infrastructure. It provides users with secure access to services required for the secondary use of health data, in compliance with the EHDS regulation.

CPL functions as the single point of access for all user interactions with other CY-EHDS-2nd modules like DAAMs and the nHDsC. The CPL is responsible for:

- Authenticating users through the national CY Login service
- Retrieving and storing immutable identity attributes (e.g. name, entity type, organisation)
- Enforcing role selection at session start, based on verified accreditation
- Providing read-only access to metadata records exposed by the national catalogue
- Enabling accredited users to access data access application interfaces
- Ensuring all access and business events are logged immutably
- Providing a secure entry point for users to submit account deletion requests in compliance with GDPR. Actual account lifecycle management is delegated to a dedicated user profile service within the CY-EHDS-2nd infrastructure, which coordinates deletion across relevant modules (DAAMs).

From a technical standpoint, CPL is implemented as a modular set of microservices deployed in containerised environments using Docker and orchestrated via Kubernetes. All services communicate internally via Representational State Transfer (REST)ful APIs documented in OpenAPI 3.0 and protected by mutual Transport Layer Security (TLS). Stateless service design allows for horizontal scalability, fault tolerance and streamlined monitoring. The same technical architecture applies to all CY-EHDS-2nd components, which are developed and deployed following a shared infrastructure pattern based on microservices, containerisation and service orchestration.

A.3.3.1 Service Layer Architecture

The CPL is structured as a set of modular, stateless microservices that operate independently and interact through secured internal interfaces. Each service is mapped to one CPL Shared Services (CPSS1–CPSS4), except where noted. In specific cases, a service may span multiple shared services or fulfil a supporting, cross-cutting function that does not correspond exclusively to a single CPSS. This modular architecture enables scalable deployment, maintainability and traceability of CPL functionalities, while enforcing separation between orchestration logic and business workflows owned by downstream components (e.g. DAAMs, nHDsC).

Each service exposes RESTful APIs documented using the OpenAPI 3.0 standard and communicates internally over secure network channels protected by mutual TLS. All session management, role enforcement and access control checks are applied before routing any request to backend modules.

The CPL services are deployed in isolated containers and orchestrated using Kubernetes, ensuring resilience, independent scaling and fault containment. The system is designed to allow horizontal scaling for high-availability scenarios and to meet the NFRs defined in Section A.3.290 of this annex.

The following internal services are implemented within CPL (Table A. 13):

Table A. 13: CY-EHDS-2nd CPL NFRs

Service Name	Mapped Shared Service	Responsibility
Authentication Gateway	CPSS1 – Identity and Access	Initiates CY Login flow, retrieves identity attributes, handles login callbacks
Session Manager	CPSS1 – Identity and Access	Manages session lifecycles, timeouts, reauthentication enforcement
Role Engine	CPSS3 – Role Management	Retrieves eligible roles, enforces session-bound role selection
Profile Service	CPSS2 – Accreditation	Displays user profile data and accreditation status
Accreditation Workflow	CPSS2 – Accreditation	Supports user submission of accreditation requests with supporting documents and enables status tracking. Accreditation decisions and workflow execution are managed externally by NeHA.
Accreditation Review Tool	CPSS2 – Accreditation	Back-office UI for NeHA officers to review, approve, or reject accreditation
Audit Logger	CPSS4 – Logging & Audit	Captures security-critical events and business actions in immutable logs
Access Routing Proxy	(Cross-cutting)	Routes authenticated, role-permitted requests to DAAMs and nHDsC modules

Each service enforces access restrictions in accordance with the user's session role, identity and accreditation status. Access control logic is applied consistently at both the API gateway and service level. Logging is integrated at each entry point, enabling full traceability and alignment with CPL audit and accountability requirements.

A.3.3.2 Interface Specifications

The CY-EHDS-2nd CPL interacts with users and external/internal systems through a set of RESTful APIs and federated authentication endpoints. All interfaces are designed in accordance with the functional and NFRs defined in previous sections. The CPL exposes and consumes only the minimum interfaces necessary to perform its orchestration, identity, role and accreditation responsibilities. Business logic and data processing are delegated to connected modules.

All exposed APIs follow the OpenAPI 3.0 specification and are protected by secure HyperText Transfer Protocol Secure (HTTPS) connections with mutual TLS enforcement. Authentication and session-level access control are applied consistently across all interfaces.

A.3.3.2.1 External Interfaces

The CPL communicates with external systems via well-defined, secure interfaces. These connections enable user authentication, metadata exploration and access application workflows, while maintaining strict boundaries between orchestration logic (CPL) and business logic (DAAMs, nHDsC).

All external interfaces are RESTful or federated (OpenID Connect), documented using the OpenAPI 3.0 specification and protected by secure HTTPS connections with mutual TLS enforcement where applicable. Authentication and access control are applied at every interaction point, based on the user's active session and role.

Table A. 14 below summarises the key external interfaces exposed or consumed by the CPL, including their technical type, direction, consumer/producer role, and purpose.

Table A. 14: External Interfaces Managed by the CPL

Interface Name	Type	Direction	Consumer/Provider	Description
CY Login Endpoint	OpenID Connect	Outbound	Provided by Government Identity Federation	Used for redirecting users to the national identity service for authentication and retrieving verified identity attributes
DAAMs API	REST (OpenAPI 3.0)	Outbound	DAAMs module (WP5)	Used to access DAAMs module to create, amend, delete or submit data access applications for authenticated data users
nHDsC API	REST (OpenAPI 3.0)	Outbound	nHDsC module (WP6)	Used to access metadata records exposed by the nHDsC for creating, updating or deleting them.by authenticated and accredited data holders or to access nHDsC metadata records for read-only viewing by public users/data users.
Internal Logging Sink	REST / File-based	Outbound	Centralised Logging Infrastructure	Interface used to stream structured audit logs to national observability infrastructure (as required by NFR4)

The CPL UI supports multilingual display for all end-user interactions, including session flows, accreditation views, and dataset catalogue exploration. All user-facing components must be presented in Greek, Turkish, or English, based on the language selected at session initiation. Metadata records retrieved from the nHDsC are displayed in the preferred session language when translations are available, otherwise, the original language version is shown.

A.3.3.2.2 Internal Interfaces

The CPL comprises a set of internal services, each exposing a minimal and secured API surface necessary to support user-facing functions and inter-service coordination. These APIs are not intended for external consumption and are accessible only within the secured CPL environment.

All internal interfaces are RESTful, documented using the OpenAPI 3.0 specification and protected via mutual TLS and internal authentication middleware. Session-based access control is enforced using signed tokens, and RBAC is applied based on the authenticated user's role.

All APIs exposed by CPL follow versioning practices and are governed by NeHA. NeHA is responsible for defining, reviewing and maintaining interface specifications across CPL, DAAMs, and nHDsC to ensure semantic interoperability and conformance to shared governance principles.

Only APIs that provide direct value to front-end components or are consumed by other CPL services are listed below. Middleware, proxy layers and back-office tools are described separately in Section A.4 and are not exposed as formal service interfaces.

Notably, administrative interfaces used by authorised NeHA back-office personnel to review and approve accreditation requests are delivered as part of an internal UI. These are not exposed as documented CPL APIs and are excluded from this specification.

All CPL APIs return structured error responses in JavaScript Object Notation (JSON) format. Each response includes:

- An HTTP status code (e.g. 400, 403, 500)
- A machine-readable error_code (such as INVALID_SESSION, UNAUTHORISED_ACCESS)
- A human-readable message that is dynamically presented in the user's session language (English, Greek, or Turkish)
- A correlation_id is included to support traceability across distributed logs.

These responses are defined in the CPL OpenAPI 3.0 specification and all failed operations are recorded in the audit log with their associated context.

A.3.3.2.3 Access Control and Session Enforcement

All interactions with CPL-protected services require users to be authenticated through the national CY Login system and to hold an active session with a declared role. Access to internal CPL services and to connected modules (e.g. DAAMs, nHDsC) is governed by RBAC policies enforced consistently at both the API gateway and service layer.

After successful login via CY Login, the CPL retrieves the user's immutable identity attributes and determines the set of eligible roles based on accreditation status. Users must explicitly select their session role before accessing any restricted functionality. The selected role governs access for the duration of the session and is used in all access control checks.

Access control is enforced using middleware components that validate the authenticity of session tokens, verify role claims and block requests to restricted routes. These middleware checks are applied to:

- All internal CPL service interfaces exposed via REST
- All routed outbound traffic to DAAMs and nHDsC via the CPL internal proxy layer

Session timeouts, re-authentication requirements and RBAC rules are applied in accordance with NFRs. All authentication attempts, session state transitions and access control decisions are recorded in the audit log for traceability and accountability.

A.3.3.2.4 Deployment and Runtime Environment

The CPL of the CY-EHDS-2nd infrastructure is deployed as a set of loosely coupled microservices, each packaged as a container image and orchestrated within a Kubernetes-managed cluster. The infrastructure will be hosted on a national platform and is operated under the responsibility of NeHA (HDAB).

The deployment model is designed to ensure operational continuity, scalability and adherence to the NFRs described in Section A.3.2. Services are isolated at the container level, enabling independent scaling, automated restarts and resilience under fault conditions. Kubernetes is responsible for health checks, load balancing, service discovery and horizontal scaling where applicable.

Each CPL service is deployed with the following baseline characteristics:

- Containerisation: All services are packaged as Docker containers with isolated runtime environments and image signing enabled for integrity.
- Service Orchestration: Kubernetes provides orchestration, readiness/liveness probes and rolling deployments across the cluster.
- Internal Networking: Service-to-service communication is encrypted using mutual TLS and managed via internal DNS.
- External Exposure: Only exposed services (e.g. Authentication Gateway, Access Control Middleware) are routed through the secured API gateway and accessed over HTTPS.
- Service Discovery: Internal services register with a Kubernetes-native service mesh to ensure dynamic routing and load balancing.

A dedicated User Profile Service manages user account lifecycle events, including GDPR-aligned deletion. While CPL provides the user-facing interface to initiate account deletion, the deletion logic is performed by the Profile Service, which coordinates downstream clean-up actions across DAAMs, nHDsC and the observability layer.

CPL handles no health data. The only persistent data it processes, such as session metadata and audit logs, is stored in secured, encrypted database systems hosted within the national environment. Accreditation documents and identity verification data are managed externally by NeHA and are not stored in CPL.

Monitoring agents and log forwarders are deployed as sidecars or embedded modules within each container. Logs, metrics and traces are streamed to the national observability infrastructure to fulfil compliance and traceability requirements. The CPL supports integration with OpenTelemetry-compatible tooling such as Prometheus, Grafana and Loki.

The CPL microservices are also designed to emit system-level events for traceability and integration purposes. These events include, but are not limited to, session creation, role selection, accreditation requests and outbound proxy actions. Events follow event-driven design patterns and are compatible with asynchronous observability and workflow integration frameworks, including Apache Kafka.

The deployment operates in a redundant active-active configuration across multiple availability zones. Disaster recovery, secure backups and replication of persistent volumes are governed by national eHealth hosting standards.

The full deployment lifecycle is managed via a CI/CD pipeline (Docker Hub - ArgoCD), which automates container builds, image scanning, integration tests and staged promotion from pre-production to production. NeHA oversees deployment governance, access control and system-level configuration in line with the CY-EHDS-2nd infrastructure governance framework.

Each CPL Shared Service (CPSS1–CPSS4) is operationally owned and governed by NeHA or its authorised infrastructure operator. This includes lifecycle management, access control policies, version updates and integration governance, ensuring alignment with national data governance frameworks.

A.3.3.2.5 Security and Compliance Measures

Security measures are embedded at every layer of the CPL stack, including authentication, session control, role validation, data persistence and audit logging. All components of the CPL are hosted in a secure, government-accredited environment. Network segmentation, infrastructure hardening and encrypted communications are enforced as part of the hosting platform.

A.3.3.2.5.1 Authentication and Identity Management

- All users must authenticate via CY Login, the national eID gateway, using the OpenID Connect protocols.
- Only identity attributes issued by the CY Login federation are accepted.
- The CPL retrieves and stores only immutable attributes required for session establishment and audit (e.g. name, legal/natural person status, organisation).
- MFA is enforced at the CY Login level for all participating actors.
- For SPE Operators, client certificate authentication is required in addition to CY Login, with certificate validation performed at the CPL ingress level.
- No local passwords, credential resets, or delegation logic are implemented within CPL.

A.3.3.2.5.2 Authentication and Identity Management

- All authenticated users must select an active session role, verified against accreditation status if applicable.
- Session timeouts, idle expiry and forced re-authentication are enforced according to NFR2.
- Session tokens are signed, traceable and stored in memory only. No persistent tokens are maintained.
- RBAC is applied uniformly across CPL services and routed components (e.g. DAAMs, nHDsC).
- All session metadata and transitions are logged in compliance with NFR4 and NFR13.

A.3.3.2.5.3 Transport and Communication Security

- All communications between CPL services occur over a Kubernetes-managed internal network with mutual TLS enforced.
- External interfaces (e.g. login flow, API gateway) are exposed only via HTTPS with TLS 1.3.
- API traffic is routed through an ingress controller that enforces origin validation, rate limiting and content inspection.
- Service-to-service calls are authenticated via mutual certificate validation and internal service accounts.

A.3.3.2.5.4 Data Confidentiality and Integrity

- The CPL does not store or process health data.
- Persistent data (e.g. audit logs, accreditation requests) is stored in encrypted data volumes.
- Backups of persistent components managed by CPL (including session metadata and audit logs) are encrypted at rest and in transit and subject to role-based access policies. CPL does not store or back up business data owned by other CY-EHDS-2nd components.
- Data integrity is verified using checksums and transaction logs at the database layer.
- Immutable logs are cryptographically protected to prevent tampering.

A.3.3.2.5.5 Auditability and Logging

- All authentication attempts, accreditation changes, session state changes and outbound application actions are recorded in structured audit logs.
- Audit logs include timestamps, user role, session ID, action performed and target component.
- Logs are streamed to a centralised national observability platform, integrated with long-term archival storage.
- Log retention policies follow GDPR and applicable national data protection law.
- Logs are accessible only to authorised system auditors and not modifiable by application services.

A.3.3.2.5.6 Legal and Regulatory Compliance

- Accreditation workflows are traceable, rule-based and subject to human validation by authorised NeHA officers.
- All processing activities by CPL are limited to metadata, session identity, accreditation data and access governance. No health data is stored or processed at any point.
- User account deletion is handled in accordance with GDPR, using a federated deletion workflow triggered via CPL and executed by the User Profile Service. Logs of deletion requests are retained for audit and regulatory compliance.
- NeHA exercises overall control of CPL operations as the designated HDAB. All processing of user metadata, accreditation submissions, session traceability and logging occurs under its legal mandate in accordance with EHDS and the national eHealth law.
- The CPL maintains an internal Record of Processing Activities (ROPA) for all personal data handling operations it performs. This includes session establishment, role selection, accreditation submission and routing of access-related actions. These records are managed under NeHA legal responsibility as the designated HDAB.

A.3.3.2.6 Scalability, Availability and Performance

The CY-EHDS-2nd CPL is designed to serve a national population of approximately 1 million citizens, as well as cross-border data users acting through the HealthData@EU infrastructure. In this context, the CPL must provide consistent response times, high availability and resilience under both normal and peak operating conditions.

The CPL is deployed as a containerised microservices architecture orchestrated by Kubernetes, with stateless services, dynamic scaling and fault isolation between components. This design supports linear scalability and predictable operational behaviour, in accordance with the NFRs.

A.3.3.2.6.1 Scalability

- All CPL services are stateless by design, allowing horizontal scaling with minimal reconfiguration.
- Kubernetes is configured to automatically scale services based on Central Processor Unit (CPU), memory and request throughput.
- Scaling policies are defined per service class (e.g. user-facing interfaces scale more aggressively than back-office tools).
- The CPL is capable of handling a minimum of 500 concurrent authenticated sessions, with scalability tested to at least 2,500 concurrent sessions under standard loads.
- All outbound communication to DAAMs and nHDsC is designed to be asynchronous and retry-safe where business logic allows.

A.3.3.2.6.2 Availability

- The CPL is deployed in a redundant active-active configuration across two physical availability zones within the national eHealth hosting infrastructure.
- Load balancing is applied at both ingress and internal service levels, using Kubernetes-native mechanisms.
- Health probes, readiness checks and liveness checks are applied to every container to ensure automated failover and restart.
- Scheduled updates are performed using rolling deployments to avoid service downtime.
- Availability target: ≥99.9% monthly uptime for all production-facing CPL endpoints.

A.3.3.2.6.3 Fault Tolerance and Recovery

- Each CPL service is independently restartable; failed containers are replaced without cascading failure.
- Application-level timeouts and circuit breakers are applied to all outbound requests to DAAMs and nHDsC modules.
- Persistent data managed by CPL, specifically session metadata and audit logs, is replicated in real time to ensure resilience and traceability. Accreditation requests and related documentation are stored and managed by NeHA and do not persist within CPL. Backups of CPL data are encrypted, integrity-checked and retained in compliance with GDPR.
- Disaster recovery procedures include regular snapshot-based backups of all persistent stores, retained in encrypted archives as per NFR4.

A.3.3.2.6.4 Performance Benchmarks

The following performance targets apply to user-facing CPL services under normal operating conditions, based on internal benchmarking and aligned with CPL-NFR6. These performance values are not contractual SLAs, but serve as design baselines to validate system responsiveness:

- User session establishment (login redirect + session role selection): target < 3 seconds
- CPL API response times (percentage (p)95): < 500 milliseconds (ms) for typical user interactions (e.g. dashboard access, profile viewing)
- Internal service-to-service latency (p95): < 100 ms (e.g. Role Engine → Profile Service)
- Audit event recording and metadata retrieval workflows: < 1 second total roundtrip under normal load

Performance thresholds are monitored continuously and serve as alert triggers in the observability platform.

A.3.3.2.6.5 Monitoring and Capacity Management

- All services are monitored using a national observability platform, with metrics collected at 15-second intervals.
- Key indicators include: request latency, CPU/memory usage, concurrent session count, queue depth and retry rate.
- Alert thresholds are defined for early degradation (e.g. latency >700ms p95, queue backlog >100 entries).
- Weekly reports are reviewed by the CPL operations team to adjust autoscaling parameters and update service limits.

A.3.3.2.7 Observability and Logging

Observability is a critical feature of the CY-EHDS-2nd CPL ensuring traceability of all user actions, system behavior and data governance operations. The CPL implements a logging, audit and metrics framework that

enables operational monitoring, compliance with legal obligations and security forensics in case of incident response.

A.3.3.2.7.1 Audit Logging

- Immutable audit logs are generated for all security-relevant and business-critical events within the CPL, including:
  - User login and logout
  - Role selection
  - Accreditation request submission
  - Access to protected service endpoints
  - Data access application proxy actions
- Audit events include:
  - Timestamp Coordinated Universal Time (UTC).
  - User session ID
  - Role
  - Target interface or operation
  - Status code (success/failure)
- Logs are write-only for CPL services and cannot be modified or deleted by runtime processes.
- Log records are pseudonymised where possible and may only be de-pseudonymised by authorised NeHA operators under strict access controls. All log access is itself logged.
- Log retention, export, and access are aligned with GDPR.
- Audit log records are signed or hashed to prevent tampering and ensure forensic validity.
- All logs are transmitted via secure channels to a centralised national observability infrastructure operated by NeHA or its designated host.

A.3.3.2.7.2 Technical Monitoring

- All CPL microservices are monitored via integrated metrics agents, collecting:
  - CPU and memory usage
  - Request count and response time (p50, p95, p99)
  - Active session count
  - Internal retry rates
  - Queue backlog for asynchronous services
- Collected metrics are pushed to a time-series database and visualised in national dashboards.
- Alerting rules are defined based on thresholds for latency, service unavailability, or resource exhaustion.

- Alerts are integrated with national incident response systems and logged as part of the operational audit trail.

The CPL monitoring architecture is designed to be compatible with widely adopted observability frameworks. Implementations may integrate tools such as Prometheus for metrics collection, Grafana for dashboards, Loki for log aggregation and Jaeger for distributed tracing. The architecture does not mandate specific tools but ensures conformance with OpenTelemetry and standard Cloud Native Computing Foundation (CNCF) observability interfaces.

A.3.3.2.7.3 Logging Infrastructure

- The CPL uses a log forwarder to transmit structured logs from each container to a secure central log sink.
- Logs are structured in JSON format and conform to a national logging schema defined by NeHA.
- Log rotation, archival and retention policies are enforced by the hosting platform.
- Logs are retained for a minimum of 5 years, in line with CPL-NFR4 and national eHealth audit requirements.
- Read access to logs is limited to authorised system operators and security officers under a defined access control policy.
- Each log entry conforms to a structured schema that includes: timestamp (UTC), session ID, correlation ID, action type, user role, system interface, operation result (success/failure) and optional subject reference. Fields are validated at log source before ingestion.
- The logging schema is versioned and centrally maintained to support backward-compatible evolution. Log consumers must declare supported schema versions.
- All logs are cryptographically signed or hash-chained at the source to ensure integrity. Tamper detection is enforced at the log sink, and alerts are generated on verification failure.

A.3.3.2.7.4 Traceability and Compliance Reporting

- A system-wide correlation ID is generated per session and propagated across CPL, DAAMs, and nHDsC service calls. This ID allows NeHA operators to reconstruct full user workflows for legal and operational analysis.
- Log correlation enables NeHA to reconstruct end-to-end workflows (e.g. accreditation request lifecycle, access request lifecycle).
- Compliance reports can be generated automatically to demonstrate adherence to auditability, retention and access governance obligations.
- Logs support export to data protection authorities upon lawful request, consistent with GDPR.

A.3.3.2.8 Account Deletion

CPL enables users to initiate account deletion requests via a secure interface, accessible only to authenticated users. The CPL does not process or store user account data directly. Instead, it forwards deletion requests to a dedicated infrastructure-level User Profile Service that governs identity-linked application data across DAAMs, nHDsC and audit logs.

The deletion process includes:

- Identity verification and session binding
- Secure API call to POST (used to submit data to a server) /user-profile/delete
- Orchestrated deletion (or pseudonymisation) of user data across modules
- Logging of deletion event for GDPR compliance

CPL receives the response status and displays it to the user. The CPL retains no data beyond session context.

A.4 CONCLUSIONS AND NEXT STEPS

The CY-EHDS-2nd General Infrastructure annex defines the foundational architecture and shared components that support the secondary use of health data in Cyprus. At the time of writing, no national infrastructure for this purpose exists, thus CY-EHDS-2nd begins from a clean slate, building a new, standards-aligned platform under the authority of NeHA, the HDAB of the Republic of Cyprus.

It sets the architectural baseline, describing the system architecture, responsibilities of the CPL and the cross-cutting shared services (CPSS1–CPSS4). It defines the orchestration logic that governs access to the five functional modules (DAAMs, nHDsC, SPE, Cross-Border Gateway and DQET) ensuring technical consistency and full compliance with the EHDS, GDPR and the Cyprus eHealth Law.

The CY-EHDS-2nd architecture is designed in line with the HealthData@EU CP specifications and related technical documentations.

A.4.1 Next Steps

Following this general infrastructure definition, the project is progressing toward the specification and implementation of the five core functional modules of CY-EHDS-2nd:

- WP5 – DAAMs
- WP6 – nHDsC
- WP7 – SPE
- WP8 – NCP and Cross-Border Gateway
- WP9 – DQET

Each of these modules is covered in a dedicated WP and will be elaborated in deliverables focusing on their requirements, pilot implementation and full operational deployment. At the same time, NeHA and the solution provider team are closely monitoring developments at the EU level, including:

- The ongoing deployment of the HealthData@EU CP
- Implementation guidance and specifications emerging from the TEHDAS2 and QUANTUM projects
- The adoption of the final Implementing Acts under the EHDS Regulation

CY-EHDS-2nd is a future-facing infrastructure and therefore the teams are committed to periodically reviewing and updating the architecture, requirements, and specifications to reflect evolving EU-level standards, national priorities and technological improvements. Where necessary, future design changes will be applied to ensure optimal alignment with EHDS and HealthData@EU expectations.

In parallel, NeHA is in the process of amending the national eHealth law to include new provisions for the secondary use of health data covering national and cross-border purposes. This legal amendment will introduce specific parameters (e.g. procedural safeguards, actor responsibilities, authorisation models) for the Republic of Cyprus to align national law with the EHDS Regulation. Once enacted, the legal updates will

trigger additional revisions to the CY-EHDS-2nd architectural design, functional requirements and governance structures to reflect the amended legal framework.

CY-EHDS-2nd is therefore not a static system but an adaptive and evolving infrastructure designed to deliver long-term regulatory compliance, technical robustness and interoperability across the EHDS.

A.5 REFERENCES

1 **European Commission, Directorate-General for Health and Food Safety (2025)**. *HealthData@EU Central Platform – Open-source Release 3: Objective, Business Requirements and Use Cases*. Luxembourg: Publications Office of the European Union, March 2025. ISBN: 978-92-68-26028-9. DOI: 10.2875/5437350.

2 **European Commission, Directorate-General for Health and Food Safety (2025)**. *HealthData@EU Central Platform – Open-source Release 3: Architecture Model and Technical Specification*. Luxembourg: Publications Office of the European Union, March 2025. ISBN: 978-92-68-26029-6. DOI: 10.2875/6472234.

3 **PwC EU Services (for DG SANTE) (2024)**. *Requirements Catalogue for Scale-Up Version (Deliverable D02.03)*. Specific Contract No. 022 under Framework Contract SLG.AVT.DI07926 – BEACON, Lot 2. European Commission, December 2024.

4 **PwC EU Services (for DG SANTE) (2024)**. *Architecture Artefacts – Scale-Up Version (Deliverable D03.03, Part 1: Architecture)*. Specific Contract No. 022 under Framework Contract SLG.AVT.DI07926 – BEACON, Lot 2. European Commission, December 2024.

5 **PwC EU Services (for DG SANTE) (2024)**. *System Specifications – Scale-Up Version (Deliverable D03.03, Part 2: System Specifications)*. Specific Contract No. 022 under Framework Contract SLG.AVT.DI07926 – BEACON, Lot 2. European Commission, December 2024.

6 **PwC EU Services (for DG SANTE) (2024)**. *Testing Framework – Scale-Up Version (Deliverable D03.03, Part 3: Testing Framework)*. Specific Contract No. 022 under Framework Contract SLG.AVT.DI07926 – BEACON, Lot 2. European Commission, December 2024.

7 **PwC EU Services (for DG SANTE) (2024)**. *ICT Governance Framework and Procedures Catalogue – Scale-Up Version (Deliverable D04.03)*. Specific Contract No. 022 under Framework Contract SLG.AVT.DI07926 – BEACON, Lot 2. European Commission, November 2024.

8 **European Parliament and Council of the European Union (2025)**. *Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847*. *Official Journal of the European Union*, L 2025/327, 5 March 2025. ELI: http://data.europa.eu/eli/reg/2025/327/oj

9 **European Commission (2025)**. *Digital Business Capabilities Blueprint*. EHDS2 Community of Practice Confluence Page, January 2025.

10 **HealthData@EU Pilot Consortium (2024)**. HealthData@EU Pilot Project Overview. Funded by the European Commission under the EU4Health Programme. Available at: https://ehds2pilot.eu

11 **TEHDAS2 Consortium (2025)**. Towards the European Health Data Space – TEHDAS2 Project Overview. Joint Action funded by the EU4Health Programme under Grant Agreement No. 101129691. Available at: https://www.tehdas.eu

12 **QUANTUM Consortium (2025)**. QUANTUM – Advancing Data Quality and Utility Labelling in the EHDS. Project funded by the European Commission under the EU4Health Programme, Grant Agreement No. 101145728. Available at: https://quantum-healthdata.eu

ANNEX B – HDAB DIGITAL BUSINESS CAPABILITIES

Table A. 15 presents the full set of HDAB DBCs defined by the EC under the EHDS regulation. Each capability is listed with its code, a functional description, its interdependencies with other DBCs, and its status regarding mandatory implementation under the EHDS and adoption within the CY-EHDS-2nd project. This structured overview is used in the project to support technical alignment, implementation planning, and regulatory compliance. Within this framework, the table in this appendix may be referenced by other deliverables of the project to link any aspect of CY-EHDS-2nd implementation to the corresponding HDAB DBCs. The table with the HDAB DBCs was developed based on official documentation and clarified further using input provided by the EC during the 2nd EHDS2 Community of Practice General Assembly (February 2025), as recorded on the EHDS2 Community of Practice confluence page.

Table A. 15: Description of the HDAB DBCs and their implementation in CY-EHDS-2nd

DBC01 - Data Holder Space	
Code	DBC01
Capability Name	Data Holder Space
Description	• Enables data holders to submit dataset descriptions to the HDAB • Includes quality and utility labels in some cases (e.g. QUANTUM) • Requires annual updates • Requires accreditation to prove metadata provider status
Dependency with other DBCs	Feeds DBC02 - Dataset Catalogue
Mandatory (EHDS)	Optional
Implemented in CY-EHDS-2nd	Yes
DBC02 - Dataset Catalogue	
Code	DBC02
Capability Name	Dataset Catalogue
Description	• Central registry where dataset descriptions are published • Allows data users to search and discover available datasets
Dependency with other DBCs	Depends on DBC01 - Data Holder Space for content
Mandatory (EHDS)	Mandatory
Implemented in CY-EHDS-2nd	Yes
DBC03 - Data User Space	
Code	DBC03
Capability Name	Data User Space
Description	• Allows users to submit data access applications (data permit or request) • Enables amendments to submitted/approved applications • Requires accreditation as a professional data user
Dependency with other DBCs	Triggers DBC05 - Data Access Application Management Space
Mandatory (EHDS)	Optional
Implemented in CY-EHDS-2nd	Yes

DBC04 - Identity Provider	
Code	DBC04
Capability Name	Identity Provider
Description	• Authenticates and authorises users and holders • Used at both national and cross-border levels
Dependency with other DBCs	• Supports DBC01 - Data Holder Space • Supports DBC03 - Data User Space
Mandatory (EHDS)	Optional
Implemented in CY-EHDS-2nd	Yes
DBC05 - Data Access Application Management Space	
Code	DBC05
Capability Name	Data Access Application Management Space
Description	• Receives applications from the Data User Space • Manages routing of applications to HDAB, data holders, or evaluation bodies • Classifies requests by type (data access, data request, amendment)
Dependency with other DBCs	• Triggered by DBC03 - Data User Space • Feeds DBC09 - Permit Issuing • Feeds DBC06 - Access Application Evaluation • Triggers DBC07 - Fees Management
Mandatory (EHDS)	Mandatory
Implemented in CY-EHDS-2nd	Yes
DBC06 - Access Application Evaluation	
Code	DBC06
Capability Name	Access Application Evaluation
Description	• Reviews scientific, societal, and ethical dimensions of applications • Can be performed by HDAB or dedicated committees • Depends on input from Application Management Space
Dependency with other DBCs	Depends on DBC05 - Data Access Application Management Space
Mandatory (EHDS)	Optional
Implemented in CY-EHDS-2nd	Yes
DBC07 - Fees Management	
Code	DBC07
Capability Name	Fees Management
Description	• Triggered by the submission of a data access request • Manages three types of fees: submission, preparation, and access assessment
Dependency with other DBCs	Triggered by DBC05 - Data Access Application Management Space
Mandatory (EHDS)	Optional
Implemented in CY-EHDS-2nd	Yes
DBC08 - Transparency Portal	

Code	DBC08
Capability Name	Transparency Portal
Description	Public portal for: • Processing results • Penalties • Opt-out procedures • Access/request decisions • Biennial HDAB reports
Dependency with other DBCs	Publishes outputs from DBC09 - Permit Issuing, DBC06 - Access Application Evaluation, and DBC15 - Supervision, Compliance & Penalties
Mandatory (EHDS)	Mandatory
Implemented in CY-EHDS-2nd	No
DBC09 - Permit Issuing	
Code	DBC09
Capability Name	Permit Issuing
Description	• Issues or revokes data permits based on access decisions • Acts as a formal approval process
Dependency with other DBCs	• Triggered by DBC05 - Data Access Application Management Space and DBC06 - Access Application Evaluation • Triggers DBC11 - Internal SPE and DBC12 - SPE
Mandatory (EHDS)	Mandatory
Implemented in CY-EHDS-2nd	Yes
DBC10 - Opt-Out Management	
Code	DBC10
Capability Name	Opt-Out Management
Description	• Allows individuals to opt out of the secondary use of their health data • Ensures opted-out data is excluded from SPE datasets
Dependency with other DBCs	Must be enforced in DBC11 - Internal SPE and indirectly in DBC12 - SPE
Mandatory (EHDS)	Mandatory
Implemented in CY-EHDS-2nd	No
DBC11 - Internal SPE (Data Preparation Environment)	
Code	DBC11
Capability Name	Internal SPE (Data Preparation Environment)
Description	• Prepares, links, and anonymises datasets after permit issuance • May generate enriched datasets for use by SPE
Dependency with other DBCs	• Triggered by DBC09 - Permit Issuing • Feeds DBC12 - SPE • Must comply with DBC10 - Opt-Out Management
Mandatory (EHDS)	Optional
Implemented in CY-EHDS-2nd	Yes

DBC12 - SPE	
Code	DBC12
Capability Name	SPE
Description	• Performs data analysis according to the permit's terms • Users extract only enriched, anonymised outputs
Dependency with other DBCs	• Depends on DBC11 - Internal SPE • Triggered by DBC09 - Permit Issuing • Must comply with DBC10 - Opt-Out Management
Mandatory (EHDS)	Mandatory
Implemented in CY-EHDS-2nd	Yes
DBC13 - SPE Operator Space	
Code	DBC13
Capability Name	SPE Operator Space
Description	• Manages accreditation and auditing of SPE operators • Provides SPE descriptions for review and approval
Dependency with other DBCs	-
Mandatory (EHDS)	Optional
Implemented in CY-EHDS-2nd	No
DBC14 - Monitoring & Reporting Management	
Code	DBC14
Capability Name	Monitoring & Reporting Management
Description	• Tracks performance indicators and produces internal reports for HDAB • Supplies inputs to Transparency Portal reports every 2 years
Dependency with other DBCs	Feeds DBC08 - Transparency Portal
Mandatory (EHDS)	Mandatory
Implemented in CY-EHDS-2nd	No
DBC15 - Supervision, Compliance & Penalties	
Code	DBC15
Capability Name	Supervision, Compliance & Penalties
Description	Enforces EHDS rules and issues penalties where necessary
Dependency with other DBCs	Feeds DBC08 - Transparency Portal
Mandatory (EHDS)	Mandatory
Implemented in CY-EHDS-2nd	No
DBC16 - Significant Clinical Findings Management	
Code	DBC16
Capability Name	Significant Clinical Findings Management
Description	Alerts individuals about health-relevant findings (unless waived)
Dependency with other DBCs	Depends on insights generated in the DBC12 - SPE
Mandatory (EHDS)	Mandatory

Implemented in CY-EHDS-2nd	No
DBC17 - Cross-Border Gateway	
Code	DBC17
Capability Name	Cross-Border Gateway
Description	• Interfaces with the HealthData@EU CP • Transmits applications, dataset metadata, KPIs, penalties, and permits
Dependency with other DBCs	Depends on information received for DBC02 - Dataset Catalogue, DBC05 - Data Access Application Management Space, DBC08 - Transparency Portal, DBC13 - SPE Operator Space
Mandatory (EHDS)	Mandatory
Implemented in CY-EHDS-2nd	Yes
DBC18 - Messaging Centre	
Code	DBC18
Capability Name	Messaging Centre
Description	• Coordinates communications across HDAB, data holders, users, and SPE operators • Especially useful for multi-country requests and findings alerts
Dependency with other DBCs	Supports DBC01 - Data Holder Space, DBC03 - Data User Space, DBC05 - Data Access Application Management Space, DBC13 - SPE Operator Space, DBC17 - Cross-Border Gateway
Mandatory (EHDS)	Optional
Implemented in CY-EHDS-2nd	No
DBC19 - Helpdesk & Incident Management	
Code	DBC19
Capability Name	Helpdesk & Incident Management
Description	• Provides support and manages complaints, objections, and incident reporting • Available to data users, data holders, and other stakeholders
Dependency with other DBCs	-
Mandatory (EHDS)	Optional
Implemented in CY-EHDS-2nd	No

ANNEX C – MAPPING OF CY-EHDS-2ND INFRASTRUCTURE TO HEALTHDATA@EU

Table A. 16: Mapping to HealthData@EU Node Architecture

HealthData@EU Node Capability	CY-EHDS-2nd Module(s)
Catalogue Interface	nHDsC (WP6)
Permit Management Interface	DAAMs (WP5)
Secure Message Handler (Domibus, AS4)	National Dispatcher for cross-border gateway (WP8)
Identity Federation Adapter	CY Login + CPL (CPSS1)
Access Control and Session Orchestration	CPL (CPSS1, CPSS3)
Logging & Audit Trail	CPL (CPSS4) → Observability Layer
Quality Metadata Provider	DQET (WP9) → Published via nHDsC (WP6)
Secure Processing Interface	SPE (WP7) (DAAMs orchestrates, but doesn't expose it)

ANNEX D – Common Actor Definitions – CY-EHDS-2nd (v1.0)

This annex defines the core actors involved in the implementation and operation of the CY-EHDS-2nd national infrastructure, spanning Work Packages 5 to 9. Each actor is described based on its formal function, regulatory basis and operational scope within the national and EU-wide architecture for secondary use of health data. All roles included in this annex correspond to actual functions and systems within the CY-EHDS-2nd ecosystem and are referenced across the deliverables D5.1 – D9.1.

The annex is aligned with the final version of the EHDS Regulation (EU) 2025/327, the official Scale-Up documentation (December 2024) and HealthData@EU CP documentation (March 2025), and reflects the architectural responsibilities defined in the CY-EHDS-2nd project design.

To ensure consistency and eliminate duplication, any mention of functional actors in this deliverable (D5.1–D9.1) must reference the official name and definition provided in this annex.

When referring to an actor, authors should:

- Use the Actor Name column exactly as listed
- Avoid rephrasing or redefining responsibilities in the main body of the deliverable
- Cite this annex as: "D5.1 Annex D: Common Actor Definitions – CY-EHDS-2nd (v1.0)

If new actors emerge during implementation that are not listed here, they must be proposed for formal inclusion after communication with the project manager.

Table A. 17: CY-EHDS-2nd Actors (across all modules)

No.	Actor Name	Definition	Actor's Responsibilities	Category	NeHA Role
A1	**General Public Citizen**	A non-authenticated visitor to the national infrastructure. This actor may access open information, such as public catalogue entries or transparency reports, but is not subject to identity verification, accreditation, or role-based access control.	• Browse the dataset catalogue • View publicly available dataset metadata • Access transparency outputs (e.g. permit decisions, KPIs) • No login or personalization required.	Human	No
A2	**Data User**	A Data User is a natural person or legal entity that seeks or has obtained access to electronic health data for secondary use, under an approved data permit or data request. Data Users must be authenticated and may be asked also to be accredited to submit applications and operate	• Submit data permit or data request applications • View and filter catalogue metadata and dataset labels • Analyze datasets in the ESPE under data permit conditions • Operate within limits of the authorized data permit	Human	No

		within SPE environments. When submitting a data access or request application, they assume the legal role of a Data Applicant as defined in Article 67 of the EHDS Regulation. Data applicants are also involved with domains data and fees associated with their requests .	scope • Receive statistical data under data request conditions • Request export of results (if applicable) • Comply with the EHDS Regulation and GDPR obligations		
A3	**Data Holder**	A Data Holder is any natural or legal person, public or private entity, institution, or organization, including health or care bodies, registries, and research centers, that has the right, responsibility, or control to make electronic health data available for secondary use. Under the EHDS Regulation, they must comply with obligations related to dataset registration, metadata provision, data availability, and quality labelling. A Trusted Data Holder is a subset of Data Holders designated by a Member State for their compliance capacity and domain expertise, with the ability to recommend application outcomes to the HDAB under simplified procedures.	• Submit dataset metadata to the National Health Dataset Catalogue (nHDsC) • Ensure metadata is accurate, up-to-date, and labelled according to EU/national standards • Respond to DQET validation feedback and revise submissions as needed • Upload requested datasets securely to the Internal SPE • Maintain timely delivery and label updates (annually or upon changes) • For Trusted Data Holders: assess and provide advisory opinions on data access applications, in accordance with Article 72 EHDS • Maintain compliance with obligations under Article 50 and 51 and, if designated, Article 72 of the EHDS Regulation.	Human	No
A4	**Application Manager**	A designated NeHA actor within the HDAB (NeHA) who oversees the intake, triage, validation, and processing lifecycle of incoming data access and request applications. The role does not evaluate the content of applications but coordinates	• Triage incoming applications and requests • Validate basic information, documentation, and applicant accreditation • Assign applications to the appropriate reviewer • Track processing status	Human	Yes

		procedural steps to ensure proper flow and completeness.	and flag incomplete or invalid submissions • Coordinate communications with applicants during processing • Finalize application status prior to permit issuance.		
A5	**Data Permit Manager**	A designated officer within the HDAB (NeHA) responsible for executing legally valid permit decisions. This actor manages the full permit lifecycle, including issuance, amendment, and revocation, based on the outcomes of application reviews and legal assessments. The role is procedural and does not involve evaluating the scientific or ethical content of applications.	• Issue permits following approval by Application Reviewers • Revoke permits upon expiry, violation, or policy grounds • Maintain permit status logs and validity information • Coordinate permit dispatch to Data Users and SPEs.	Human	Yes
A6	**Application Reviewer**	An evaluator authorized by the HDAB (NeHA) who is responsible for assessing data permit and data request applications. The reviewer performs in-depth analysis of each application's legal, scientific, and ethical dimensions, based on Article 67 of the EHDS Regulation.	• Review the application purpose, proportionality, and safeguards • Assess compliance with EHDS, GDPR, and ethical standards • Request amendments or clarifications from applicants • Record review findings and recommendation • Contribute to permit acceptance or rejection decisions.	Human	Yes
A7	**nHDsC Manager**	The nHDsC Manager is a designated HDAB (NeHA) actor responsible for overseeing the national Health Dataset Catalogue (nHDsC). This role ensures that validated dataset metadata and associated labels are published, maintained, and	• Publish validated metadata and labels into the nHDsC • Oversee metadata lifecycle management • Initiate synchronization with HealthData@EU CP catalogue	Human	Yes

		synchronized with the HealthData@EU Central Platform. The nHDsC Manager is accountable for metadata version integrity, publication scheduling, and coordination with other HDAB functions related to nHDsC.	• Coordinate actions related to dataset description publication (e.g. with DQET Manager and nHDsC Auditor)		
A8	**nHDsC Auditor**	The nHDsC Auditor is an actor designated by the HDAB (NeHA) responsible for the semantic, structural, and compliance validation of dataset metadata records submitted to the National Health Dataset Catalogue. This role acts as a quality gate before publication, ensuring all records conform to Health DCAT-AP specifications, national catalogue rules, and expected interoperability standards. The Auditor does not directly approve or reject records but reports findings to the nHDsC Manager.	• Validate metadata structure and semantics according to Health DCAT-AP • Verify compliance with national metadata publication standards • Identify missing or invalid fields • Flag non-compliant records and return findings to the nHDsC Manager • Maintain audit trail of validations performed	Human	Yes
A9	**DQET Manager**	A DQET Manager is a NeHA-authorized quality officer who validates and manages data quality and utility labels associated with dataset metadata. The role ensures that label content complies with national rules and European frameworks (e.g. QUANTUM), and that feedback to Data Holders is properly recorded and actioned.	• Review and assess submitted dataset labels • Approve, reject, or revoke labels • Request clarifications or amendments from Data Holders • Initiate updates if compliance issues arise • Record decisions in the system audit log	Human	Yes
A10	**Internal SPE Operator**	An authorized NeHA staff member with privileged access to the Internal Secure Processing Environment (ISPE). This actor is responsible for receiving and preparing data for permitted	• Receive data uploads from Data Holders via secure SFTP • Perform data processing (e.g. pseudonymization, harmonization) • Transfer prepared	Human	Yes

		processing operations involving direct handling of raw or sensitive data in the context of a data permit or data request.	datasets to the ESPE (for data permits) • Log and version datasets and outputs • Deliver statistical results to Data Users (for data requests)		
A11	**ESPE Operator**	A system or personnel role responsible for managing the ESPE infrastructure accessible to authorized Data Users. This actor provisions the environment per data permit requirements and ensures compliance with usage policies.	• Provision and configure ESPE per data permit • Enforce technical safeguards (e.g. encryption, no internet) • Monitor session duration and activity • Revoke access upon expiration or policy breach • Provide secure environment for analysis using pre-approved tools	System	Yes
A12	**System Administrator**	A NeHA technical operator responsible for managing the backend infrastructure and security configuration of the national infrastructure components. This role supports but does not participate in data access workflows.	• Maintain system infrastructure and uptime • Manage logs and audit trails • Configure authentication services and access layers • Perform updates and security patching • Support incident resolution	Human	Yes
A13	**HDAB Business Owner / Solution Provider**	The HDAB Business Owner is the institutional actor within NeHA responsible for the strategic oversight, legal compliance, and full-lifecycle governance of the CY-EHDS-2nd national infrastructure. As the designated HDAB of Cyprus under the EHDS Regulation and national law, NeHA assumes this role to ensure lawful, secure, and interoperable secondary use of health data.	• Define and maintain the service governance model • Set operational priorities for DAAMs, nHDsC, SPE, connection with HealthData@EU CP and data quality enhancement toolbox modules • Oversee national compliance with EHDS and GDPR obligations • Assign roles and coordinate HDAB personnel	Human (Institutional Actor)	Yes

A14	**HealthData @EU CP**	The EC's centralized system component responsible for cross-border data exchange between Member State HDABs and authorized participants. It handles submission, routing, and receipt of dataset descriptions, applications, permits, and other relevant messages. Operates via the Domibus eDelivery infrastructure.	• Receive and publishes dataset descriptions from national catalogues • Facilitate submission and reception of cross-border data access applications by the Member States • Transmit permit decisions and notifications between Member States • Enable secure, structured communication across HDAB nodes • Log and track transactional data for auditing purposes	System	No
A15	**DAAMs**	The Data Access Application Management system (DAAMs) is a national CY-EHDS-2nd software component responsible for managing the full lifecycle of data access and statistical request applications. It coordinates the user interface, form submission, validation logic, and internal workflow routing to NeHA-assigned roles.	• Accept and validate incoming applications • Coordinate procedural tasks between Application Manager, Reviewer, and Permit Manager • Record workflow status and timestamps • Trigger updates to relevant modules (SPE, DQET, nHDsC) upon permit issuance • Interface with the National Dispatcher for outbound cross-border exchanges	System	Yes
A16	**nHDsC**	The National Health Dataset Catalogue (nHDsC) is the central metadata registry of CY-EHDS-2nd. It stores, manages, and publishes structured descriptions of datasets made available for secondary use. The catalogue supports quality labels, search and filtering, and synchronization with the EU platform.	• Store and version dataset metadata and labels • Enable metadata validation workflows with nHDsC Auditor and DQET Manager • Publish searchable dataset entries to national users • Synchronize catalogue exports to the HealthData@EU CP • Provide metadata access via public and role-based views	System	Yes
A17	**Internal SPE**	The ISPE is a restricted, non-user-facing component of the CY-EHDS-2nd infrastructure. It is managed by NeHA and used for	• Receive datasets from Data Holders • Apply permit-defined transformations (e.g.	System	Yes

		secure data handling, preparation, and transformation prior to user access or cross-border dispatch.	pseudonymization, aggregation) • Transfer results to ESPE or deliver statistical outputs • Log and version each processing activity		
A18	**ESPE**	The ESPE is the secure, user-facing data analysis environment provisioned to authorized Data Users under permit. It supports data exploration using pre-approved tools and operates under strict technical and legal safeguards.	• Launch permit-specific SPE environments • Enforce access control policies (e.g. time-limited sessions, no internet) • Provide toolsets and software within the SPE • Monitor use and ensure compliance with permit terms • Revoke access automatically or upon violation	System	Yes
A19	**National Dispatcher**	The National Dispatcher is a technical middleware component that facilitates structured message exchange between CY-EHDS-2nd modules and the HealthData@EU CP. It ensures messages are compliant, signed, and transmitted over Domibus.	• Receive outbound messages from DAAMs or nHDsC • Apply national signing and packaging rules • Transmit dataset descriptions and data permits to the HD@EU CP via Domibus • Receive inbound cross-border applications from the HD@EU CP • Log communication events for auditability	System	Yes
A20	**Domibus Gateway**	The Domibus Gateway is the underlying eDelivery channel used by the National Dispatcher and HealthData@EU CP to exchange structured EHDS-compliant messages. It ensures secure, authenticated, and standards-based transmission of permit requests, metadata, and notifications.	• Support AS4-compliant transmission of messages • Authenticate endpoints and ensure encryption • Manage message queues and delivery retries • Enable logging and error handling for cross-border communication	System	Yes
A21	**DQET**	The Data Quality and Utility Toolbox (DQET) is the national module responsible for managing dataset quality assessment workflows. It	• Enable label self-assessment submission by Data Holders • Coordinate validation workflows with DQET	System	Yes

		supports label self-assessments, validation, and governance for quality and utility indicators.	Manager • Record label versioning, status, and decisions • Trigger re-validation upon label changes • Interface with nHDsC for publishing label content		

ANNEX E – CY-EHDS-2ND KEY TERMINOLOGY

This annex presents a consolidated glossary of key terms used across the CY-EHDS-2nd deliverables (D5.1 to D9.1). The listed terms were selected based on their actual usage within these deliverables. Their definitions are grounded in the official documentation of the HealthData@EU CP and the validated outputs (milestones) of the TEHDAS2 Joint Action (up to May 2025), and have been reviewed for consistency with the final version of the EHDS Regulation, (EU) 2025/913 of the European Parliament and of the Council of 13 March 2025 on the EHDS.

This glossary ensures conceptual clarity and regulatory alignment and is intended to support the consistent interpretation of core terminology across the national implementation of the EHDS in Cyprus.

Table A. 18: CY-EHDS-2nd Key Terminology

No.	Term	Definition	Synonyms
T1	**Access Logging Service**	A technical service that records every access and operation performed on sensitive data within the Secure Processing Environment. It supports accountability, transparency, and auditability.	Logging mechanism, audit service
T2	**Accreditation Mechanism**	A national or EU-level system that verifies and certifies entities (data users, researchers, institutions) for eligibility to access health data for secondary use under the EHDS.	–
T3	**Anonymization**	The process by which personal data is irreversibly altered so that a data subject can no longer be identified, directly or indirectly. Anonymized data is not considered personal data under the GDPR.	Anonymous data
T4	**Benefit**	Refers broadly to positive outcomes of data use, including health, social, and environmental improvements. It is used in evaluating the public value of secondary health data use.	Public benefit
T5	**Catalogue Entry**	A metadata record describing a dataset, its access conditions, variables, provenance, and data controller. Each entry in the dataset catalogue represents a unique dataset available for secondary use.	Dataset metadata record
T6	**Central Platform Layer (CY-EHDS-2nd)**	The national component of the CP infrastructure that provides shared services (e.g., identity federation, role enforcement) for Cyprus. It ensures alignment with the EU CP while integrating national systems like CY Login.	CPL
T7	**Central Platform (HealthData@EU)**	The EU-level platform coordinated by the EC that enables cross-border cooperation between Health Data Access Bodies. It provides metadata discovery, request routing, and shared services for secondary data use.	HealthData@EU CP
T8	**Community of Practice**	A group of professionals and stakeholders who collaboratively share practices, guidelines, and experiences to advance semantic and technical aspects of health data infrastructure, such as metadata standardization or quality frameworks.	–
T9	**Completeness (Quality)**	The degree to which all required data elements are present in a dataset. One of the six dimensions of quality defined in the QUANTUM project.	–

T10	**Consistency (Quality)**	The degree to which data values are harmonized and logically aligned within and across datasets.	–
T11	**Controlled vocabulary**	A standardized set of terms used to ensure consistency in data labeling, aiding discoverability, interoperability, and semantic clarity (e.g., code lists, ontologies).	–
T12	**Data access**	Processing by a data user of data that has been provided by a data holder, in accordance with specific technical, legal, or organizational requirements, without necessarily implying transmission or downloading.	–
T13	**Data discoverability**	The degree to which datasets and their characteristics can be located and identified through catalogue services and metadata. A prerequisite for effective data access.	–
T14	**Data Holder**	An entity, person, or organization that holds and controls electronic health data, and may make it available for secondary use in accordance with the EHDS.	Health data holder
T15	**Data Interoperability Layer**	A technical framework within the infrastructure enabling data exchange between systems and components through common standards and APIs.	Interoperability Layer
T16	**Data Minimization**	A GDPR principle requiring that only data which is strictly necessary for the specific purpose is collected and processed.	–
T17	**Data Permit**	A formally approved authorization (issued via the health data access application process) that specifies the conditions under which health data may be accessed and processed. A data permit is managed through the project's DAAMs and is identified by a unique permit ID. It governs all data flows and operations in an SPE, ensuring compliance with specified technical and organizational requirements.	–
T18	**Health Data Access Application**	The formal application process through which an individual or organization requests secondary use of health data under the EHDS. This process is managed by the project's DAAMs and yields, upon approval, a data permit or data request with a unique reference ID.	Data Access Application, Application
T19	**Data Processing**	Any operation or set of operations performed on personal data, whether or not by automated means, such as collection, storage, retrieval, use, disclosure, or erasure.	Processing activity
T20	**Data Provenance**	Information about the origin, context, and transformation of a dataset. Provenance enhances transparency, trust, and data quality.	Dataset history
T21	**Data Quality**	The fitness of a dataset for its intended use. In QUANTUM, data quality is defined across six dimensions: completeness, accuracy, consistency, timeliness, accessibility, and interpretability.	–
T22	**Data Request**	A formally approved request for a statistical output or aggregated result derived from health data. Unlike a data permit (which grants analytical access to data within an SPE), a data request results in predefined statistical results delivered to the requester without providing raw data or direct SPE access.	–

T23	**Data Sharing**	Provision by a data holder of data to a data user for the purpose of joint or individual use of the shared data, based on agreements, directly or via intermediaries.	–
T24	**Data Subject Rights**	Rights granted under the GDPR to individuals concerning their personal data, including access, rectification, erasure, and objection.	–
T25	**Data User**	A natural person or legal entity seeking to access health data for secondary use purposes under EHDS (e.g., research, policymaking, innovation). Must meet eligibility criteria.	Health data user
T26	**Dataset**	A structured collection of data, typically organized for a specific purpose such as analysis, access, or sharing. Datasets are described by metadata and subject to access conditions under EHDS.	–
T27	**Dataset Description**	The structured metadata describing a dataset within the national dataset catalogue. Includes source, scope, key characteristics, and access conditions. Required by Article 77 of the EHDS Regulation.	Metadata record
T28	**Dataset Quality Assessment**	The process and methodology for evaluating a dataset against agreed quality dimensions. Implemented via the DQET in CY-EHDS-2nd.	Quality evaluation
T29	**EU Dataset Catalogue**	A centralized EU-level repository aggregating dataset metadata received from Member State catalogues via the NCPs. It facilitates discoverability across borders.	Central metadata repository
T30	**FAIR Principles**	A set of guiding principles to improve the Findability, Accessibility, Interoperability, and Reusability of digital assets. Applied to metadata and datasets under EHDS.	–
T31	**HealthData@EU**	The EU-wide infrastructure established under EHDS to support the secure cross-border exchange and secondary use of health data. It comprises a network of Health Data Access Bodies and a CP operated by the EC.	HealthData@EU infrastructure
T32	**Health Data Applicant**	A natural or legal person submitting a data access application or a data request to a HDAB for purposes under EHDS Article 53.	–
T33	**Interoperability**	The ability of different systems, organizations, or components to exchange and use information effectively. This includes legal, organizational, semantic, and technical dimensions.	–
T34	**Logging Service**	See: Access Logging Service	Audit service
T35	**Metadata**	Structured information that describes, explains, or enables the discovery, access, use or management of a dataset. Metadata enhances dataset discoverability and reuse.	–
T36	**Metadata Catalogue**	A structured repository that stores metadata records about datasets, supporting discovery, access, and reuse of health data.	Dataset catalogue
T37	**Metadata Record**	See: Dataset Description	–
T38	**Personal Data**	Any information relating to an identified or identifiable natural person. Includes names, IDs, location data, or factors specific to physical, genetic, mental, economic, cultural or social identity.	Individual-level data

T39	**Non-Personal Data**	Data that does not relate to an identified or identifiable natural person. This includes anonymized data or data about populations/statistics.	Anonymous data, statistical data, aggregated data
T40	**Pseudonymization**	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 information is kept separately and subject to technical and organizational safeguards. It reduces identification risks while preserving utility for data analysis.	–
T41	**Public Value**	A weighted assessment of the expected benefits and risks of data use, considering fairness, harm mitigation, sustainability, and long-term societal value.	–
T42	**Quality Dimensions**	Refers to the aspects used to evaluate data quality, including completeness, accuracy, consistency, timeliness, interpretability, and accessibility.	Data quality dimensions
T43	**Role Enforcement Service**	A component of the Central Platform Layer responsible for ensuring that users' access roles align with the permissions granted via the data permit.	–
T44	**Secondary Use**	The processing of health data for purposes other than those for which the data were originally collected, as defined in Chapter IV of the EHDS Regulation.	–
T45	**Semantic Interoperability**	The ability of systems to automatically interpret the meaning of exchanged data based on agreed vocabularies and ontologies, ensuring shared understanding across contexts.	–
T46	**Secure Processing Environment (SPE)**	A controlled infrastructure with certified safeguards ensuring lawful, secure, and privacy-preserving processing of sensitive data. SPEs enforce audit logging, isolation, and role-based access controls, in line with GDPR and EHDS obligations. Includes internal subcomponents (ISPE for ingestion and ESPE for analysis).	Trusted environment, Secure environment
T47	**Shared Services**	Common services offered by the Central Platform Layer (CPL), including logging, identity federation, accreditation routing and role enforcement.	–
T48	**Timeliness (Quality)**	The degree to which data is current and up to date for its intended purpose.	–
T49	**Data User (Authorized Applicant)**	A person or legal entity explicitly named in an approved data permit (or data request) who is granted access to the processed health datasets or outputs. Data users may be researchers, statisticians, or other analysts approved to enter the ESPE and perform analysis. They must follow all SPE usage rules and can only access data and functions permitted by their data permit.	–
T50	**ESPE**	A virtualized, user-specific secure workspace provisioned for authorized data users under a data permit. The ESPE hosts only the prepared dataset linked to the permit and includes pre-installed analytical tools. It is accessed via CY Login with 2FA and strictly forbids data download or external connectivity.	–

T51	**ISPE**	The backend component of the SPE architecture used by the HDAB to ingest, prepare, and transform datasets provided by data holders. It supports secure upload (e.g. via SFTP), logging, and transformation before release to the ESPE.	–
T52	**CY Login**	The Cyprus national eID single sign-on system used to authenticate data users accessing the ESPE. It provides strong identity verification (with 2FA) and integrates with the Central Platform Layer.	–
T53	**2FA**	A security method requiring users to provide two independent forms of identification (e.g. password and one-time code) to log in. Mandatory for ESPE access.	Two-factor authentication
T54	**SFTP**	A network protocol that provides secure (encrypted) file transfer. Used by data holders to upload datasets to the SPE (typically to the ISPE component) in compliance with data permit specifications.	–
T55	**EHDS (Regulation)**	The EU framework regulating the secondary use of health data across Member States. Sets rules for HDABs, SPEs, permits, access, data subject rights, and cross-border flows. Official title: *Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 March 2025 on the EHDS*.	–