



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

Proposal number: 101129405

D8.1 National Connector for Cross-border gateway Requirements and Specifications

(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
Maria	Papaioannou	Cyprus	University of Cyprus (UCY)	Affiliated Entity (AE)
Ioannis	Rodosthenous	Cyprus	UCY	AE
Waqar Aziz	Sulaiman	Cyprus	UCY	AE
Constantinos	Pattichis	Cyprus	UCY	AE

Reviewed by

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

Abbreviations

AE	Affiliated Entity
API	Application Programming Interface
AS4	Applicability Statement 4
CA	Competent Authority
COO	Coordinator
CP	Central Platform
CP R3	Central Platform Release 3
CPL	Central Platform Layer
CY-EHDS-2nd	European Health Data Space for Secondary Use @CY
DAAMs	Data Access Application Management solution
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EC	European Commission
EHDS	European Health Data Space
EU	European Union
FRs	Functional Requirements
HDAB	Health Data Access Body
HealthDCAT-AP	Health Data Catalogue Vocabulary Application Profile
ITB	Interoperability Test Bed
JSON	JavaScript Object Notation
mTLS	mutual Transport Layer Security
NCP	National Contact Point
ND	National HealthData@EU Dispatcher
NeHA	National eHealth Authority
NFRs	Non-Functional Requirements
nHDsC	National Health Dataset Catalogue
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
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
UCY	University of Cyprus
WP	Work Package
WS	Web Service
XBDE	Cross-Border Data Exchange
XBG	Cross-Border Gateway
XML	eXtensible Markup Language

Executive Summary

This deliverable, D8.1: National Connector for Cross-Border Gateway (XBG) – Requirements and Specifications, defines the foundational architecture and technical requirements of Work Package (WP) 8 of the European Health Data Space for Secondary Use @CY (CY-EHDS-2nd) project¹. WP8 implements the national Cross-Border Data Exchange (XBDE) infrastructure for the Republic of Cyprus, enabling the country to participate in the European Health Data Space (EHDS)² for the secondary use of health data, in full alignment with the EHDS Regulation European Union (EU) 2025/327 and the specifications of the HealthData@EU³ Central Platform Release 3 (CP R3)⁴.

WP8 serves as the technical realization of the National Contact Point (NCP) for Secondary Use. Its responsibilities include:

- Outbound transmission of structured metadata about nationally available datasets (from the national Health Dataset Catalogue – (nHDsC), WP6) and approved data access permits (from the Data Access Application Management solution (DAAMs), WP5).
- Inbound processing of cross-border data access applications and requests submitted through the HealthData@EU CP by EU-authorized users, ensuring correct routing to relevant national systems.

The XBDE architecture is modular and comprises of two key sub-components:

- National HealthData@EU Dispatcher (ND), which orchestrates internal communication, transforms and validates data and constructs outbound Applicability Statement 4 (AS4) messages.
- Domibus-based XBG, the secure AS4 interface to the HealthData@EU network, responsible for message-level transmission and reception, in compliance with the EU eDelivery standard.

This deliverable provides:

- A detailed description of the legal and regulatory context (Chapter 2), including all relevant provisions of the EHDS Regulation.
- An overview of how XBDE aligns with the HealthData@EU CP R3 model (Chapter 3).
- A modular technical architecture, including sub-component responsibilities, data flow analysis and integration points with national systems and shared services (Chapter 4).
- A catalogue of functional and Non-Functional Requirements (NFR) (Chapter 5), covering interoperability, security, traceability, maintainability and future extensibility.

The scope of implementation in CY-EHDS-2nd WP8 includes only those data flows currently supported by HealthData@EU CP R3: dataset publication, application reception, and permit issuance. However, WP8 is explicitly designed to support additional flows (e.g. permit status updates, Secure Processing Environment (SPE) metadata) as soon as technical specifications become available at the EU level.

The design incorporates adaptability to align with forthcoming EHDS Implementing Acts and outputs from Second Joint Action Towards the European Health Data Space (TEHDAS2)⁵ ensuring WP8 remains a compliant and effective component of the evolving EHDS.

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://op.europa.eu/en/publication-detail/-/publication/65b5ad44-0ac7-11f0-b1a3-01aa75ed71a1/language-en>

⁵ <https://tehdas.eu/>

Table of contents

1

INTRODUCTION

4

1.1

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

4

1.1.1

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

4

1.1.1.1

Annex A – CY-EHDS-2nd Architecture and Central Platform (CP) Infrastructure

4

1.1.1.2

Annex B – HDAB Digital Business Capabilities

5

1.1.1.3

Annex C – Indicative Mapping to HealthData@EU CP Infrastructure

5

1.1.1.4

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

5

1.1.1.5

Annex E – CY-EHDS-2nd Key Terminology

5

1.1.2

Recommended Reading Order

5

1.2

D8.1 Introduction

6

1.3

Objective of the Deliverable

6

1.4

Connection with other CY-EHDS-2nd Work Packages

6

1.5

Interconnections

8

2

LEGAL FRAMEWORK

9

2.1

European Health Data Space Regulation (EU 2025/327)

9

2.2

National legal framework

10

3

ALIGNMENT WITH HEALTHDATA@EU CP

11

3.1

The HealthData@EU CP R3 Model for Data Exchange

12

4

ARCHITECTURE OF THE CY-EHDS-2ND INFRASTRUCTURE FOR CROSS-BORDER DATA EXCHANGE FOR SECONDARY USE

14

4.1

High-Level Architecture

15

4.2

XBDE Interaction with HealthData@EU Central Platform Infrastructure

15

4.3

XBDE Interaction with other CY-EHDS-2nd modules

17

4.4

XBDE Sub-Component Architecture

18

4.5

National HealthData@EU Dispatcher

18

4.5.1

Core Responsibilities

18

4.5.2

Deployment and Integration

19

4.6

Domibus-based Cross-Border Gateway

19

4.6.1

Key Responsibilities and Operations

20

4.6.2

Deployment and Integration

21

4.7

XBDE as the Technical Implementation of National Contact Point Functionalities

21

4.8

Data Flows

22

4.9

Outbound Data Flows

22

4.9.1

Outbound Flow: Dataset Catalogue Synchronization to HealthData@EU CP

23

4.9.2

Outbound Flow: Data Permit Issuance

25

4.9.2.1	Outbound Flows: Future	26
4.10	Inbound Data Flows	26
4.10.1	Inbound Flow: Reception of New or Amended Data Access Applications from HealthData@EU CP	27
5	REQUIREMENTS AND SPECIFICATIONS	28
5.1	Functional Requirements.....	28
5.2	General Cross-Border Requirements	29
5.3	National HealthData@EU Dispatcher Requirements.....	30
5.4	Cross-Border Gateway (Domibus) Requirements.....	32
5.5	Non-functional Requirements.....	33
5.6	WP8NFRC1 - Performance Efficiency	33
5.7	WP8NFRC2 - Interoperability	35
5.8	WP8NFRC3 - Reliability.....	36
5.9	WP8NFRC4 – Security	37
5.10	WP8NFRC5 – Maintability.....	39
5.11	WP8NFRC6 – Compliance	41
6	CONCLUSIONS AND NEXT STEPS.....	42
6.1	Next Steps.....	43
7	References.....	43

List of Figures

Figure 1: CY-EHDS-2nd National Dispatcher for CrossBorder Gateway module (as implemented by WP8)	7
Figure 2: HealthData@EU Communication between a NCP and the HD@EU CP [3-7].....	12
Figure 3: System in Context [1-2].....	13
Figure 4: AS4 Message Flow [1-2]	14

List of Tables

Table 1: Outbound Cross-Border Data Flows from Cyprus to HealthData@EU CP	23
Table 2: Dataset Catalogue Synchronization to HealthData@EU CP Actors as defined in <i>D5.1 Annex D: Common Actor Definitions – CY-EHDS-2nd (v1.0)</i>	24
Table 3: Data Permit Issuance Actors as defined in <i>D5.1 Annex D: Common Actor Definitions – CY-EHDS-2nd (v1.0)</i> ..	25
Table 4: Future Outbound Flows	26
Table 5: Inbound Cross-Border Data Flows from HealthData@EU CP to Cyprus	27
Table 6: Reception of Data Access Applications from HealthData@EU CP Flow Actors as defined in <i>D5.1 Annex D: Common Actor Definitions – CY-EHDS-2nd (v1.0)</i>	28
Table 7: General Cross Border FRs.....	29
Table 8: ND FRs	30
Table 9: XBG Functional Requirements	32
Table 10: Overview of the NFRs Categories of XBDE	33
Table 11: WP8 - NFR - Performance Efficiency	34
Table 12: NFR - Interoperability.....	35
Table 13: NFR – Reliability.....	36
Table 14: NFR – Security	38
Table 15: NFR – Maintainability.....	39
Table 16: NFR – Compliance	41

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 WPs, 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 Central Platform (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, nHDSs, DAAMs, SPE, National Connector and Quality Toolbox, are interconnected through a central coordination layer (the Central Platform 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 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 community of practice 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 Central Platform (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 Toolbox Requirements and Specifications
6. D7.1 – SPE: Requirements and Specifications
7. D8.1 – National Connector for XBG Requirements and Specifications

1.2 D8.1 Introduction

This deliverable specifies the requirements and architectural specifications of the national connector for the XBG infrastructure to be developed under CY-EHDS-2nd WP8. It outlines how Cyprus will implement its NCP role for the secondary use of health data, in full alignment with the EHDS Regulation (EU 2025/327) and the technical specifications of the HealthData@EU CP R3.

The CY-EHDS-2nd WP8 infrastructure, referred to herein as the XBDE module, enables Cyprus to securely, reliably and compliantly participate in the HealthData@EU network, by managing all inbound and outbound cross-border data flows for dataset metadata, data access applications and data permits. This module is developed from scratch as part of the CY-EHDS-2nd national infrastructure and acts as the regulated interface between the national components and the HealthData@EU CP.

Figure 1 presents the overall CY-EHDS-2nd logical interactions between actors and the national infrastructure modules as well as the data communication between the functional modules. The modules and interactions implemented under WP8 are colored in blue line.

1.3 Objective of the Deliverable

The objective of this deliverable is to define the functional and NFRs, technical architecture, interoperability points and integration specifications for the implementation of the XBDE module. This deliverable focuses strictly on the flows that are technically supported in Release 3 of the HealthData@EU CP and are included in the scope of CY-EHDS-2nd, namely:

- Publication of dataset metadata on Health Data Catalogue Vocabulary Application Profile (HealthDCAT-AP⁶) Resource Description Framework (RDF)
- Reception of cross-border data access applications
- Synchronisation of issued data permits
- Future readiness for permit lifecycle and status updates, pending EU interface definitions

The XBDE will be the only pathway through which Cyprus exchanges secondary-use health data with the EU-level infrastructure and, as such, must operate in accordance with strict technical, legal and operational standards. The specifications herein will serve as the foundation for XBDE pilot and production implementations (Deliverables D8.2 and D8.3).

1.4 Connection with other CY-EHDS-2nd Work Packages

WP8 is tightly integrated with the broader CY-EHDS-2nd infrastructure, particularly the following WPs:

- WP5 – DAAMs: Provides application and permit lifecycle management. All cross-border data access applications and data permits are received by and processed within DAAMs. WP8 infrastructure transmits and receives structured JavaScript Object Notation (JSON) representations of these elements. More information on CY-EHDS-2nd DAAMs can be found in *D5.1 DAAMs Requirements, Specifications and Prototype* deliverable.
- WP6 – nHDsC: Manages the creation and publication of dataset descriptions. WP8 infrastructure retrieves approved RDF records from the nHDsC for transmission to the HealthData@EU CP. The deliverable *D6.1 nHDsC Requirements and Specifications* includes information on the requirements and specifications of the CY-EHDS-2nd nHDsC.

⁶ <https://healthdcap.github.io/>

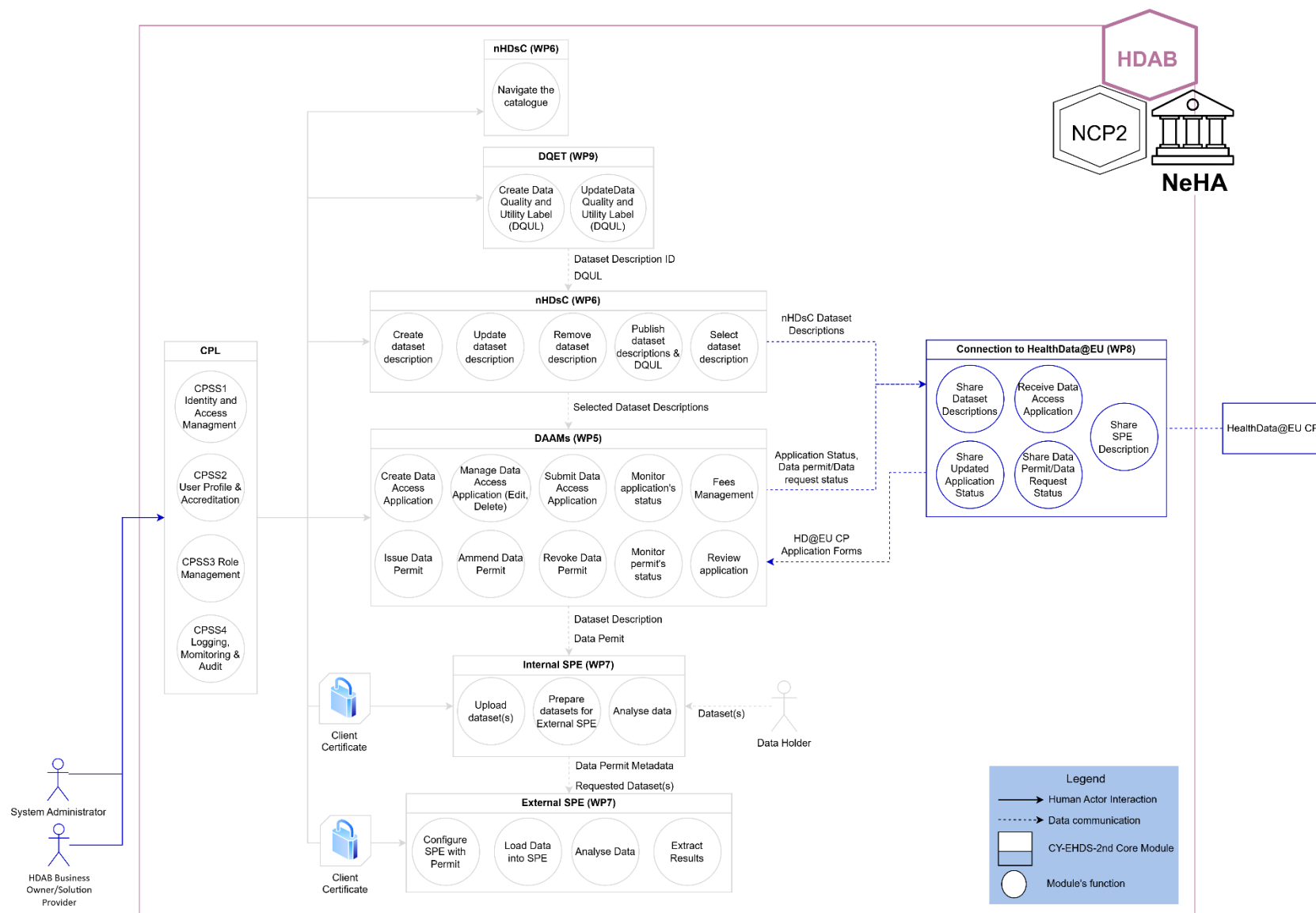


Figure 1: CY-EHDS-2nd National Dispatcher for CrossBorder Gateway module (as implemented by WP8)

1.5 Interconnections

The XBDE module operates as a tightly coupled yet modular component within the CY-EHDS-2nd national infrastructure. To perform its mandated role as the NCP interface for secondary health data use, it must coordinate with multiple national subsystems and shared service layers. These interconnections are fundamental to ensuring secure, seamless and standards-compliant end-to-end cross-border data flows.

- **DAAMs (WP5)**

The DAAMs component is the primary recipient of inbound data access applications and requests arriving via XBDE. It also serves as the source for outbound messages concerning data permit issuance and where technically supported in the future for application status or data permit/request lifecycle updates (e.g. permit revocation). The National Dispatcher fetches application or permit information from DAAMs through internal Application Programming Interfaces (APIs) and notifies DAAMs upon successful inbound reception from the HealthData@EU CP. More information on the CY-EHDS-2nd DAAMs can be found in *D5.1 DAAMs Requirements, Specifications and Prototype* deliverable.

- **nHDsC (WP6)**

XBDE interconnects with the nHDsC to retrieve approved and published dataset descriptions for outbound transmission to the HealthData@EU CP. These metadata records must be provided in RDF format according to HealthDCAT-AP standards. The National Dispatcher fetches the required dataset record using internal API calls initiated when the nHDsC Manager triggers a synchronization event. More information on the CY-EHDS-2nd nHDsC can be found in *D6.1 nHDsC Requirements and Specifications* deliverable.

- **CPL**

Offers core cross-cutting services such as identity and access management (CPSS1), user profile management (CPSS2), Role-based access control (RBAC) (CPSS3) and audit logging (CPSS4), all of which are leveraged by WP8 infrastructure for secure operations. More information on the CY-EHDS-2nd CPL can be found in *D5.1 Annex A: CY-EHDS-2nd Architecture and CP Infrastructure*.

- **Shared Database Infrastructure**

XBDE uses the national data storage cluster for persisting operational metadata, transaction states, AS4 acknowledgments and system configuration details. More information on the CY-EHDS-2nd Shared Database Infrastructure can be found in *D5.1 Annex A: CY-EHDS-2nd Architecture and CP Infrastructure*

- **Shared Observability Stack**

All key events processed within XBDE, such as message reception, dispatch, transformation, and AS4 status codes, are logged with structured metadata into the CY-EHDS-2nd shared observability platform. This ensures traceability, enables root-cause analysis for errors and supports audit trails required under the EHDS Regulation and national governance policies. More information on the CY-EHDS-2nd Shared Observability Stack can be found in *D5.1 Annex A: CY-EHDS-2nd Architecture and CP Infrastructure*.

- **CI/CD Automation Pipeline**

XBDE source code, configurations, and deployment artefacts are integrated into the CY-EHDS-2nd CI/CD automation framework. This enables consistent, repeatable and secure deployments across environments (development, testing, staging and production), with automated testing, quality checks and rollback procedures. More information on the CY-EHDS-2nd CI/CD Automation Pipeline can be found in *D5.1 Annex A: CY-EHDS-2nd Architecture and CP Infrastructure*

- **Configuration and Secrets Management**

All XBDE components, including the Dispatcher and Domibus instance, retrieve operational parameters, certificates, and credentials from the shared CY-EHDS-2nd configuration and secrets management system. This ensures secure handling of sensitive data (e.g. API keys, Transport Layer Security (TLS) certificates) and allows the National eHealth Authority (NeHA) to centrally manage configurations with traceability and policy enforcement. More information on the CY-EHDS-2nd Configurations and Secrets Management can be found in *D5.1 Annex A: CY-EHDS-2nd Architecture and CP Infrastructure*.

2 LEGAL FRAMEWORK

The development and implementation of the XBDE module under CY-EHDS-2nd is guided by a dual legal framework comprising EU-level legislation, primarily the EHDS Regulation and the evolving national legal framework of the Republic of Cyprus. XBDE serves as the national technical infrastructure enabling Cyprus to fulfill its obligations as a Member State within the European HealthData@EU ecosystem for the secondary use of electronic health data.

2.1 European Health Data Space Regulation (EU 2025/327)

Regulation (EU) 2025/327 on the EHDS [8] establishes the legal foundation for the secondary use of electronic health data across the EU. It defines a harmonized legal and technical framework to enable lawful, secure, and interoperable access to health data for purposes such as research, innovation, policy-making, official statistics, public health, patient safety and regulatory supervision.

WP8 implements key cross-border exchange functions of the Cypriot NCP for secondary use as defined in the EHDS Regulation. The following provisions are of direct relevance:

- **Designation and Role of NCPs**

The EHDS Regulation requires each Member State to designate one or more NCPs for Secondary Use. WP8 constitutes the technical realization of this function for Cyprus, enabling structured interaction with the HealthData@EU CP.

- **EU Dataset Catalogue Synchronization**

The EHDS Regulation, NCPs must ensure that information about available electronic health datasets is continuously and systematically provided to the HealthData@EU infrastructure, using the common metadata model adopted for this purpose. WP8 is responsible for enabling this obligation technically, by collecting approved dataset metadata from the national catalogue (WP6 – nHDsC), transforming it into the HealthDCAT-AP format, and publishing it to the HealthData@EU CP via AS4 messaging. This flow is fully supported in HealthData@EU CP R3 and implemented as part of CY-EHDS-2nd.

- **Cross-Border Data Access Mechanisms**

The Regulation introduces a pan-European mechanism for data users in one Member State to request access to datasets hosted in another, coordinated via the NCPs and HealthData@EU. XBDE is responsible for receiving such requests addressed to Cyprus and supporting the transmission of outbound information as permitted.

- **Secure Communication Infrastructure**

EHDS mandates the use of secure and interoperable communication infrastructure. WP8 complies by implementing the eDelivery AS4 protocol using Domibus, the EU-endorsed solution for message-level security, integrity and reliability.

- **Logging and Monitoring of Processing Operations**

EHDS requires that all processing operations carried out by NCPs be comprehensively logged. WP8 integrates with the CY-EHDS-2nd observability platform to ensure auditability of message transmission, receipt, transformation and routing operations, in alignment with this requirement.

- **Interoperability and Standardization**

The Regulation imposes requirements for semantic and technical interoperability. WP8 adheres to these mandates by implementing support for HealthDCAT-AP, eDelivery AS4 messaging and other specifications defined in the HealthData@EU CP R3 documentation [1-2].

- **Security and Data Protection**

EHDS emphasizes security, confidentiality, and safeguards during secondary data processing and transmission. WP8 is designed to implement secure communication channels (AS4 over TLS), mutual authentication, message integrity and comprehensive logging aligned with both the EHDS and the General Data Protection Regulation (GDPR)⁷.

- **Transparency and Oversight**

The Regulation introduces obligations for transparency in NCP operations, including the publication of permit information. NCP must be capable of supporting such reporting needs where applicable, even if not all flows are in scope during CY-EHDS-2nd implementation.

- **Role and Limitations of the HealthData@EU CP**

EHDS clarifies that the HealthData@EU CP acts solely as a metadata routing infrastructure and does not store or process the actual content of datasets. WP8 ensures that all transmissions comply with this separation of responsibilities, transmitting only metadata and administrative information, not raw health data.

The architecture and requirements defined in Chapters 4-5 of this deliverable are directly informed by these obligations. WP8 is being designed to be fully compliant with the EHDS Regulation and to remain adaptable as future Implementing Acts and technical specifications are published.

2.2 National legal framework

The operation of XBDE and the broader CY-EHDS-2nd infrastructure for the secondary use of health data will be governed by the national legal framework of the Republic of Cyprus, in conjunction with the overarching EU regulations (EHDS Regulation, GDPR).

Currently, the existing national eHealth Law provides a comprehensive framework for the primary use of electronic health data and established the NeHA as the CA. However, specific provisions detailing the governance, procedures and technical requirements for the secondary use of health data, particularly concerning cross-border exchange and connection with infrastructures like HealthData@EU, are not yet explicitly codified within the current national legislation. It is anticipated that an amendment to the national

⁷ <https://gdpr-info.eu/>

eHealth law will be undertaken to address these aspects comprehensively. This forthcoming amendment is expected to (among other provisions) provide the national legal grounding for the technical infrastructure being established, including WP8 and its connection to the HealthData@EU CP. Until this amendment is enacted, the design and implementation of WP8 will proceed based on the direct applicability of the EHDS Regulation and GDPR, and in close consultation with the Health Data Access Body (HDAB) (NeHA) to ensure alignment with anticipated national legal interpretations and future legislative provisions. All functionalities of XBDE will be designed to be adaptable to the specific requirements that will emerge from the amended national eHealth law⁸.

3 ALIGNMENT WITH HEALTHDATA@EU CP

A foundational principle for the design and operation of WP8 is its complete technical and operational alignment with the HealthData@EU CP, as detailed in its Release 3 documentation [1-2] (and subsequent binding updates). The HealthData@EU CP establishes the common European infrastructure, services, technical specifications and governance for the cross-border secondary use of health data under the EHDS Regulation. WP8, acting as the NCP interface of Cyprus, must seamlessly integrate with this CP.

This alignment is based on the following essential aspects, which are elaborated throughout the technical specifications of this deliverable:

- **Adherence to Technical Specifications:**

WP8 must implement and strictly adhere to the technical specifications published by HealthData@EU CP for National Nodes. This includes the mandated eDelivery AS4 profile for secure message exchange, the specific Processing Mode (PMode) configurations for interaction with the HealthData@EU Central Domibus, defined API interaction patterns for the National Dispatcher (where applicable) and any other technical prerequisites for participation in the HealthData@EU network.

- **Compliance with Data Formats and Semantics:**

WP8 must ensure that all data exchanged with the HealthData@EU CP conforms to the specified data formats and semantic standards. This primarily involves:

- Using HealthDCAT-AP (the health-specific extension of DCAT-Application Profile for data portals in Europe) for describing and exchanging dataset metadata.
- Utilizing the standardized JSON schemas defined by HealthData@EU CP for data access applications, permit information and status updates.

- **Utilization of HealthData@EU Services and Tools:**

CY-EHDS-2nd, through WP8, will leverage services and tools provided by the HealthData@EU CP where applicable. This includes utilizing the HealthData@EU Interoperability Test Bed (ITB) and official validators (e.g. HealthDCAT-AP validator) for conformance testing and ensuring the correctness of data exchanges.

⁸ [https://www.neha.org.cy/en/legislation/#:~:text=59\(1\)%2F2019%20is,the%20Electronic%20Health%20Record%20and](https://www.neha.org.cy/en/legislation/#:~:text=59(1)%2F2019%20is,the%20Electronic%20Health%20Record%20and)

- Participation in Governance and Operational Procedures:**

The operation of WP8 must align with the governance framework and operational procedures established for the HealthData@EU network. This may include adherence to common processes for onboarding, incident management and updates to technical specifications.

This commitment to deep alignment ensures that WP8, as the Cypriot NCP, functions as a reliable and fully interoperable node within the wider HealthData@EU ecosystem, enabling Cyprus to effectively participate in the EHDS for the secondary use of health data. All functional, non-functional and technical specifications detailed in this document for WP8 are developed with this primary alignment goal of conforming to the HealthData@EU CP R3 requirements.

However, it is important to note that only the subset of cross-border message types that are technically implemented in R3 of the HealthData@EU CP (i.e. dataset metadata, applications, requests, and permit issuance) are currently supported at the European level. CY-EHDS-2nd will implement this core functionality and is also prepared to support additional flows such as permit status updates and revocations, provided the relevant technical specifications are made available by the HealthData@EU CP in time. Other flows (e.g. SPE metadata, sanctions, or KPIs reporting) are acknowledged as future requirements and will be addressed outside the scope of CY-EHDS-2nd.

3.1 The HealthData@EU CP R3 Model for Data Exchange

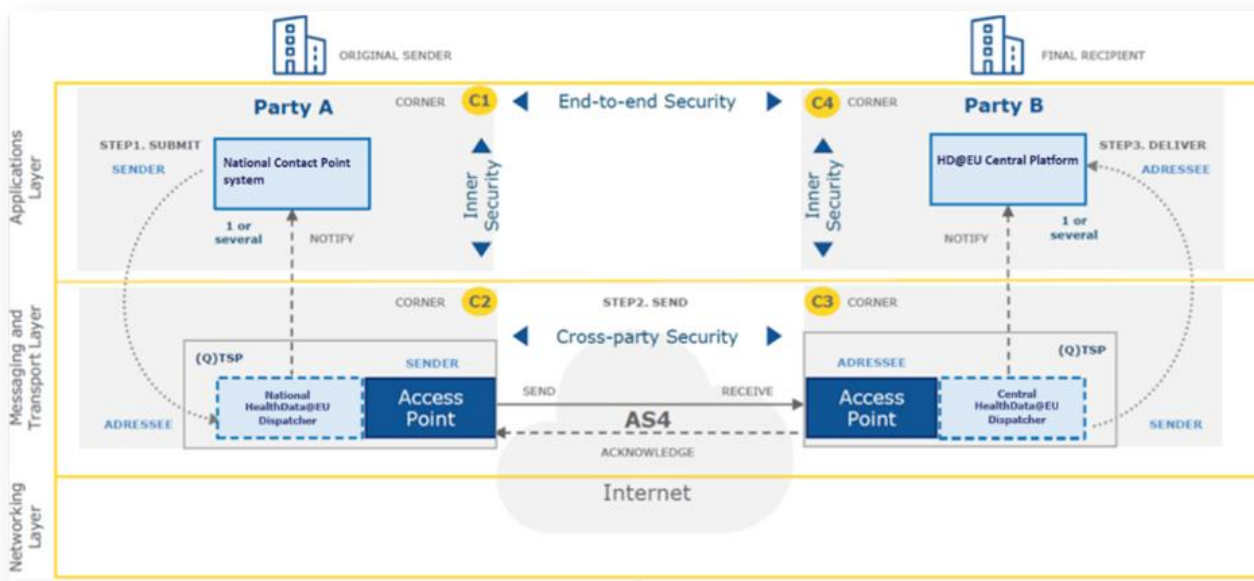


Figure 2: HealthData@EU Communication between a NCP and the HD@EU CP [3-7]

Typical cross-border message exchange between the NCP and the HealthData@EU CP uses the eDelivery AS4 protocol. The Cypriot national connector (WP8) supports exactly the scenarios prescribed by the HealthData@EU CP R3 reference architecture, acting as the intermediary in these secure AS4 exchanges. In outbound scenarios (NCP towards HealthData@EU CP), WP8 forwards dataset catalogue records and data permits / data requests (e.g. after application approval) from the national DAAMs and nHDsC to the EU CP. In inbound scenarios (HealthData@EU CP towards NCP), it receives data access applications and related notifications sent by EU users via the HealthData@EU CP. All such interactions use the four-corner AS4 model (C1/C4 back-end systems, C2/C3 access points as depicted in Figure 2, with the WP8 ND mediating the

payload before it reaches the Cypriot National Domibus for outbound messages and the HealthData@EU Central Dispatcher mediating the payload after receipt by the Central Domibus for inbound messages, as per the Release 3 design.

This alignment with the HealthData@EU reference architecture and interfaces, as illustrated in Figure 3, guarantees that the Cyprus NCP will interoperate correctly with the HD@EU CP. In particular, the implementation follows the cross-border infrastructure architecture (connectivity via eDelivery AS4) and integration scenarios (message flows to/from HD@EU CP) as defined in the R3 deliverables, ensuring that all data exchanges conform to the mandated protocols and processes.

The relevant diagrams in the HD@EU CP architecture document illustrate how national HealthData infrastructures connect to the EU platform via the standard eDelivery (AS4) framework. In each figure below (Figure 3 & Figure 4), we quote the official caption and then describe the workflow, identify the main components (e.g. National/central gateways, dispatchers, contact points) and explain how the diagram clarifies the XBDE process.

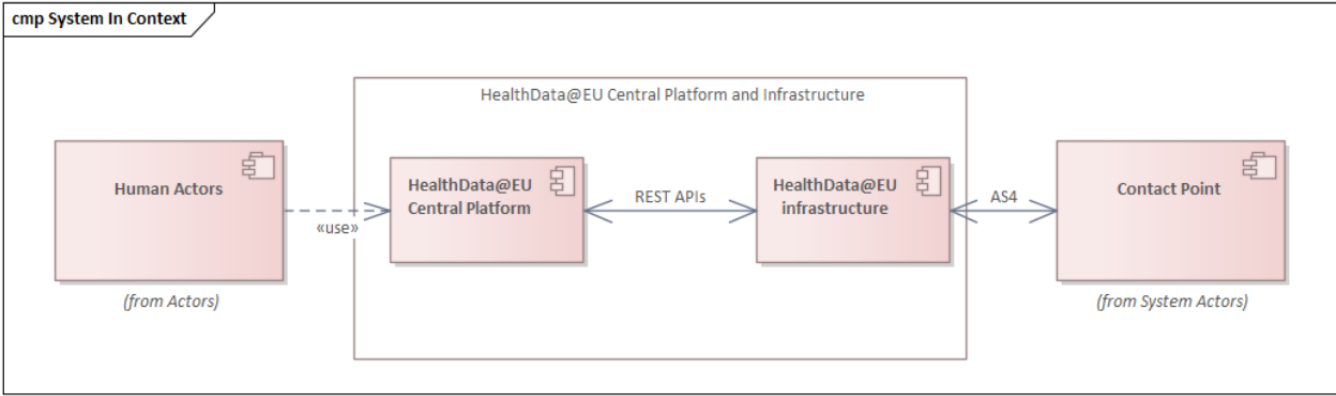


Figure 3: System in Context [1-2]

This contextual diagram, reflecting the HealthData@EU CP R3 Conceptual Architecture Overview, situates the HealthData@EU CP within the overall EHDS ecosystem. It shows the CP (with its dataset catalogue, data access repository, etc.) at the center and depicts its connections to national infrastructures and external actors. Key components include the HealthData@EU CP, its Central AS4 Gateway (Central Domibus) and multiple Member State NCPs, each with their own AS4 gateway (National Domibus) and ND. The figure also shows these NCPs or connectors in each country, which act as local eDelivery hubs. By drawing arrows between the Central Domibus and each National Domibus (AS4 gateway), the diagram makes clear that all cross-border messages travel over the Commission’s eDelivery network.

The figure indicates that each Member State will have one XBG instance (one per NCP) to exchange data with the Central Services. As the HealthData@EU CP R3 architecture specifies, these gateways all use the standard eDelivery (AS4) protocol. In the figure, arrows from national nodes (NCPs) to the CP represent exactly these AS4-based channels. Thus, Figure 4 depicts that the CP is not isolated: it is part of a network of nodes, each using Domibus-based gateways to communicate over AS4. This high-level view emphasizes that all XBDE (dataset updates, permit status, etc.) flows via these gateway connectors rather than through ad hoc links. WP8, as the Cypriot NCP, implements one such national node, utilizing its Domibus-based gateway and ND.

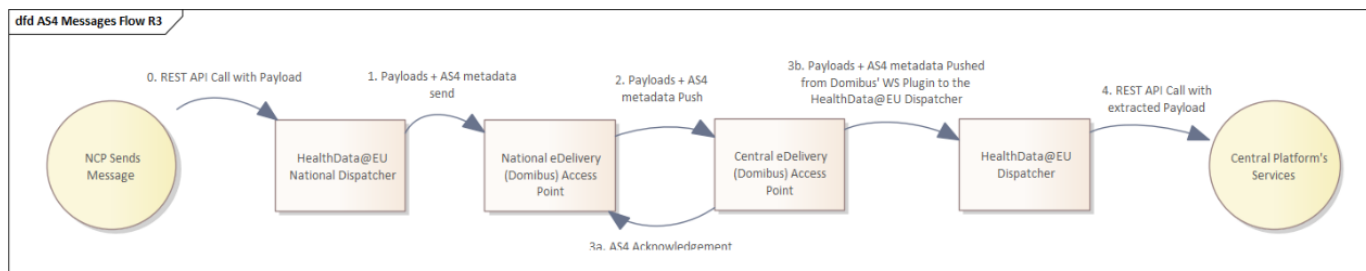


Figure 4: AS4 Message Flow [1-2]

Figure 4, illustrating a typical AS4 transaction from a national system to the HealthData@EU CP (as per R3 documented flows), shows how WP8 components fulfill the national roles: The Cypriot NCP submits a payload (e.g. dataset metadata or permit information) to the WP8 ND (the Cypriot software component implementing this R3-defined role). The WP8 National Dispatcher then packages the payload in an AS4 Message with the recipient as the Central Domibus. The next component is the Cypriot National AS4 Gateway (National Domibus): the WP8 National Dispatcher hands the AS4 message to this gateway. The Cypriot National Domibus instance then pushes the message to the HealthData@EU infrastructure Central Domibus. Once the Central Domibus receives the AS4 message, it automatically returns an eDelivery receipt acknowledgment (per the AS4 profile) to the Cypriot National Domibus. The Central Domibus then uses its Web Service (WS) plugin to forward the decrypted payload to the HealthData@EU Central Dispatcher. Finally, the Central Dispatcher unpacks the payload and delivers it to the appropriate HealthData@EU CP module (e.g. the Piveau Catalogue Dataset Record Repository, Health Data Access service). In summary, the components shown as fulfilling the national roles include: the National bodies (data sender within Cyprus), the WP8 ND, the Cypriot National Domibus gateway (NCP); and on the central side, the Central Domibus gateway, and the HealthData@EU Central Dispatcher/Services. By laying out these steps, the figure makes the cross-border exchange process explicit: data originating in a Member State travels through the standard eDelivery nodes to reach the central system. The use of AS4 (as mandated by R3) is highlighted, the Cypriot national gateway (XBDE Domibus instance) uses the AS4 protocol (Domibus implementation) to ensure secure, standards-based delivery. As noted in official HealthData@EU CP R3 documentation, Domibus is the reference AS4 access point implementation used for these gateways.

The architectural mechanisms and message handling roles described here are implemented within the XBDE architecture as detailed in Chapter 4. This includes the ND, Domibus Gateway, and their API bindings to WP5 (DAAMs) and WP6 (nHDSsC).

4 ARCHITECTURE OF THE CY-EHDS-2ND INFRASTRUCTURE FOR CROSS-BORDER DATA EXCHANGE FOR SECONDARY USE

Chapter 4 presents the architecture of the XBDE infrastructure developed under WP8 of the CY-EHDS-2nd project. The XBDE is the national technical implementation that enables Cyprus to act as a NCP within the HealthData@EU infrastructure, specifically for the secondary use of health data across borders.

The architecture is designed in full alignment with HealthData@EU CP R3, adopting the prescribed message formats, communication protocols, and component interfaces. The XBDE is responsible for securely exchanging dataset catalogue records, data access applications, data requests, and data permits with the CP, using the Domibus-based eDelivery AS4 messaging infrastructure.

The chapter describes the overall architectural context, the main components of the XBDE infrastructure, and their interactions with other CY-EHDS-2nd modules. It also outlines the direction of data flows and the scope of implementation covered within this deliverable.

4.1 High-Level Architecture

The XBDE module is a cornerstone of the CY-EHDS-2nd infrastructure, specifically designed to manage all outbound and inbound XBDE activities related to the secondary use of health data. It enables Cyprus to securely and efficiently share a defined set of data categories, including dataset metadata and data requests and permit decisions with the HealthData@EU CP.

XBDE is also responsible for receiving and processing incoming messages, such as cross-border data access applications originating from the HealthData@EU CP. While the current scope of R3 limits the types of supported message exchanges, the XBDE architecture is designed to be extensible. It will accommodate additional flows such as application status, permit status updates (e.g. revoked) and SPE descriptions when formal specifications become available at EU level.

At a high level, XBDE functions as a controlled and auditable conduit, abstracting the complexities of cross-border communication protocols, primarily AS4 messaging over eDelivery via Domibus, from the core national modules, including the nHDsC WP6 and the DAAMs, WP5. The system includes mechanisms to detect relevant data or status changes in these modules that require cross-border action or notification.

The XBDE architecture is built on the principles of modularity, security, interoperability, and full alignment with the reference architecture defined in HealthData@EU CP R3. It leverages EU-standard technologies where applicable and adheres strictly to the technical and semantic standards mandated for participation in the HealthData@EU ecosystem. The XBDE architecture is built on the principles of modularity, security, interoperability, and full alignment with the reference architecture defined in HealthData@EU CP R3. It leverages EU-standard technologies where applicable and adheres strictly to the technical and semantic specifications required for participation in the HealthData@EU ecosystem. All interactions are governed by the overarching CY-EHDS-2nd CPL for essential services such as authentication, session management and high-level audit logging, the details of which are described in the deliverable *D5.1 Annex A: CY-EHDS-2nd Architecture and CP Infrastructure* and are referenced herein where appropriate.

4.2 XBDE Interaction with HealthData@EU Central Platform Infrastructure

The XBDE module ensures that Cyprus can securely and effectively communicate with the HealthData@EU CP in compliance with the protocols, payload formats and roles defined in R3 version. This interaction enables XBDE for secondary use, supporting both outbound and inbound flows such as dataset synchronisation, data access application intake, and permit issuance.

Communication between XBDE and the CP follows a layered architecture, consisting of two key components:

1. The Domibus-based XBG

This gateway serves as the AS4-compliant transport layer for cross-border messaging. It uses the eDelivery network to exchange messages with the Central Domibus node of the HealthData@EU CP. The National Domibus instance in Cyprus is configured with the required WS Plugin to:

- Transmit outbound AS4 messages generated by the XBDE Dispatcher
- Receive inbound AS4 messages pushed by the Central Domibus

- Ensure secure transmission and reception with acknowledgements, retries, and delivery receipts

2. The HealthData@EU National Dispatcher

This is the core application-level interface of XBDE. It performs the following tasks:

- Exposes secure Representational State Transfer (REST) APIs to national systems (e.g. DAAMs, nHDsC)
- Validates incoming and outgoing payloads (RDF or JSON)
- Converts validated payloads into base64-encoded AS4 messages
- Logs message metadata and transmission status
- Triggers message delivery via the XBG
- Handles incoming AS4 messages and delivers them to national endpoints

All communication with the CP is asynchronous and fully auditable. The National Dispatcher avoids polling by relying on push mechanisms configured in the Domibus WS Plugin, which notifies the Dispatcher upon message arrival or status change.

The types of message exchanges supported in this configuration are defined by the HealthData@EU CP Release 3 and include:

- **Outbound flows:** dataset creation or update or deletion, data permit or data request synchronization
- **Inbound flows:** data access applications and data requests (including amendments)

Additional flows such as permit status updates, revocations, and SPE metadata are not yet technically supported by the CP but are foreseen as future extensions. XBDE has been designed to accommodate these flows when formal message specifications become available.

While the XBDE is fully aligned with the HealthData@EU CP R3 and will support all message types that are technically implemented at EU level, certain additional cross-border flows foreseen in the EHDS regulation and referenced in scale-up documentation [3-7] are not yet supported in Release 3. These include:

- Data Access Application status updates
- Lifecycle events related to issued permits (e.g. expiration, renewal, etc.)
- SPE metadata
- Publication of penalties applied
- Publication of KPIs

These flows are acknowledged as future compliance targets, and the XBDE architecture is designed to support their integration once corresponding message types and interfaces are formally defined at EU level. Internal XBDE components will log relevant events and support auditability where appropriate, but no cross-border transmission for these flows is foreseen during CY-EHDS-2nd.

4.3 XBDE Interaction with other CY-EHDS-2nd modules

Within the CY-EHDS-2nd national infrastructure, XBDE plays a pivotal role in connecting domestic secondary use of health data processes with the European HealthData@EU ecosystem. It achieves this through defined interactions with other key national modules, primarily the CPL, the nHDsC (WP6) and the DAAMs (WP5).

Key interaction patterns with national modules include:

- **Interaction with the CPL**

XBDE itself does not directly interface with end-users for authentication or session management. Any administrative interfaces for XBDE configuration or monitoring (if required by NeHA operators) would be accessed via the CPL, which handles user authentication (via CY Login), session management, and RBAC. Details of CPL services are outlined in the deliverable *D5.1 Annex A: CY-EHDS-2nd Architecture and CP Infrastructure*.

XBDE components contribute to the centralized audit logging system managed via the CPL, ensuring that all cross-border transaction events (e.g. message sending/reception, status changes, errors) are securely and immutably logged for traceability and compliance, in line with CPSS4 (Logging, Monitoring, and Audit).

- **Interaction with nHDsC - WP6**

The nHDsC maintains the structured metadata describing health datasets available for secondary use. When a new dataset is created or an existing one is updated and approved by the HDAB nHDsC Auditor, the HDAB nHDsC Manager can manually trigger a synchronization action.

This triggers the export of the dataset description in RDF format (HealthDCAT-AP), which is sent to XBDE via its REST API. XBDE validates the RDF payload, generates the corresponding AS4 message, and transmits it through Domibus to the HealthData@EU CP catalogue component.

This workflow ensures that cross-border data users have timely access to searchable, standardized dataset metadata originating from Cyprus.

- **Interaction with DAAMs - WP5**

The DAAMs is responsible for receiving, processing, and managing data access applications and data requests at the national level. When a cross-border application is received via the HealthData@EU CP, XBDE ingests the AS4 message, decodes the payload, and passes the structured application content to DAAMs via its secure REST API.

Once a data access application is evaluated and approved by the HDAB Application Manager, the resulting data permit or data request decision is synchronized back to the CP through XBDE. DAAMs prepares the decision payload in the required JSON format and transmits it to XBDE, which packages and sends the permit to the HealthData@EU CP using the Domibus eDelivery infrastructure. The XBDE also supports future notification flows (e.g. application status updates or permit lifecycle changes), which will be enabled once formal message types are defined and implemented by the CP.

Critical Error Event Publication by XBDE:

XBDE publishes critical operational error events (e.g. related to Domibus connectivity, persistent message processing failures) to designated topics on the shared event bus for consumption by the central Monitoring/Alerting System.

- **General Principles for Internal Interactions (API and Event-Driven):**

Internal API interactions (e.g. CY-EHDS-2nd National Dispatcher fetching full data from nHDsC/DAAMs) adhere to RESTful principles, are documented using OpenAPI 3.0, and are secured using mechanisms defined by the CY-EHDS-2nd shared infrastructure (e.g. mutual Transport Layer Security (mTLS)).

Data exchange formats for API payloads are aligned with the needs of XBDE for onward cross-border transmission (e.g. nHDsC provides HealthDCAT-AP RDF, DAAMs provides status information in a structured format mappable to EU-specified JSON).

These API-based internal interactions ensure that XBDE can effectively and resiliently gather necessary information from national sources for EU-level exchange and correctly route incoming EU communications, all while maintaining clear architectural boundaries and leveraging shared CPL and event bus services.

4.4 XBDE Sub-Component Architecture

The XBDE infrastructure consists of modular and interoperable subcomponents that implement the technical responsibilities of Cyprus as a NCP within the HealthData@EU infrastructure. Each sub-component plays a defined role in preparing, transforming, and transmitting messages to and from the HealthData@EU CP in full compliance with the R3 specifications. This section describes the internal architecture and functional role of each subcomponent, including their responsibilities, interfaces, and integration points with the broader CY-EHDS-2nd system.

4.5 National HealthData@EU Dispatcher

The ND (hereafter “National Dispatcher”) is the core application-layer component of the XBDE infrastructure. It acts as the central orchestration and processing hub for all cross-border messages, handling both outbound flows to the HealthData@EU CP and inbound messages received from the CP via Domibus.

Designed for full alignment with the specifications defined in HealthData@EU CP R3, the National Dispatcher ensures that all data exchanged between Cyprus and the European infrastructure is validated, securely packaged, reliably transmitted and auditable in accordance with EU and national requirements.

4.5.1 Core Responsibilities

1. Internal API Exposure

The National Dispatcher exposes secure internal REST APIs, consumed by DAAMs (WP5) and nHDsC (WP6), to initiate cross-border messaging operations. These APIs conform to OpenAPI 3.0 specifications and implement CY-EHDS-2nd security policies.

2. Payload Preparation and Validation

It receives structured data payloads from internal systems (e.g. RDF for datasets, JSON for data permits) and validates them against the HealthData@EU schemas. Validation includes syntax, format, and semantic consistency.

3. Message Transformation and Packaging

Validated payloads are transformed into AS4-compliant messages. This includes:

- Base64 encoding of payloads

- Insertion of message metadata (e.g. sender/receiver identifiers, message properties)
- Preparation of envelope headers in line with eDelivery profiles

4. Outbound Message Delivery

Outbound messages are handed off to the National Domibus (WP8 XBG), which handles the secure AS4 transmission to the CP. The Dispatcher tracks submission attempts and records outcomes.

5. Inbound Message Handling

Messages received from the HealthData@EU CP, such as data access applications, are pushed by the Domibus WS Plugin. The Dispatcher unwraps the AS4 envelope, validates the payload and delivers it to the correct internal system (e.g. DAAMs).

6. Acknowledgement and Status Tracking

The Dispatcher processes technical acknowledgments from Domibus, including:

- RECEIPT (successful delivery acknowledgment)
- ERROR (failure during transmission)

It maintains message lifecycle logs and updates message states accordingly (e.g. sent, acknowledged, failed).

7. Error Handling and Retry Logic

The Dispatcher implements configurable retry mechanisms for transient failures (e.g. temporary API unavailability or message queuing errors). Critical errors are logged with enriched metadata to support operational troubleshooting.

8. Audit Logging and Compliance

In compliance with CPSS4 of the CY-EHDS-2nd CPL, the Dispatcher produces detailed audit logs for all processing stages. These logs include timestamps, payload references and message state transitions and are made available to the national observability and compliance stack.

4.5.2 Deployment and Integration

The Dispatcher is deployed within the national hosting environment and integrated with other CY-EHDS-2nd services via secure internal APIs. It communicates with:

- National Domibus via Simple Object Access Protocol (SOAP) (WS Plugin)
- DAAMs and nHDsC via REST
- CPL services for logging, authentication, and role enforcement

The Dispatcher is stateless and designed to support asynchronous communication. It includes extensibility hooks for future support of new message types (e.g. permit revocations, SPE metadata) as soon as they are defined by the EU infrastructure.

4.6 Domibus-based Cross-Border Gateway

The Domibus-based XBG is the transport-layer component of the XBDE infrastructure, responsible for the secure and reliable exchange of AS4 messages between the National Dispatcher and the HealthData@EU CP via the European eDelivery network.

This gateway implements the Domibus software stack, which is the EC's reference implementation of the eDelivery AS4 protocol. It is configured in accordance with the specifications defined in HealthData@EU CP R3 and includes a WBs Plugin that supports asynchronous, event-driven message exchange. The XBG component also operates as a stateless, standards-compliant message transport layer. Its integration with the National Dispatcher ensures that all cross-border exchanges are handled securely, efficiently and in full alignment with the interoperability specifications defined by the HealthData@EU CP.

4.6.1 Key Responsibilities and Operations

1. Secure AS4 Message Exchange

The Gateway ensures secure message transmission using the AS4 protocol, including:

- Message signing and encryption (per eDelivery AS4 profile)
- WS-Security header handling
- TLS-based transport with mutual authentication

2. Interface with the National Dispatcher

- **Outbound:** The National Dispatcher submits fully packaged AS4 messages (including payloads like RDF datasets or JSON applications) to Domibus for cross-border transmission.
- **Inbound:** Messages received from the Central Domibus are processed by the Gateway and handed off to the National Dispatcher. The interaction is implemented via the Domibus WS Plugin, which is configured to push messages upon arrival or status change.

3. eDelivery Network Compliance

The Gateway is configured in accordance with the HealthData@EU eDelivery operational profile. This includes:

- **PMode configuration** (files) defining sender/receiver rules, transport protocols, security policies
- Management of **cryptographic credentials**, supported cipher suites, and certificate exchange
- Compliance with HealthData@EU participation requirements

4. Message Reliability and Non-Repudiation

Domibus provides delivery guarantees through:

- Acknowledgements (RECEIPT) for every transmitted message
- Error signaling (ERROR) in case of failures
- Non-repudiation of origin (NRO) and Non-repudiation of receipt (NRR), using AS4 headers and logs

5. Logging and Monitoring

All AS4 transport events, including submission, delivery, acknowledgment, and errors—are logged within the Domibus instance. Where feasible, these logs are integrated into the shared CY-EHDS-2nd observability stack governed by the CPL (CPSS4), ensuring traceability and auditability across all cross-border exchanges.

6. Configuration and Governance

The XBG is configured and operated under the authority of NeHA or its designated technical operators. Configuration responsibilities include:

- Maintaining up-to-date PMode files and trust anchors
- Managing WS Plugin settings, including push endpoints and retry rules
- Ensuring synchronization with HealthData@EU CP updates

Secure operations of the Gateway are essential to maintaining Cyprus compliance with the HealthData@EU trust framework and ensuring interoperability with other Member States.

4.6.2 Deployment and Integration

The Domibus-based XBG is deployed within the secure hosting environment managed by NeHA (NCP). It is installed and maintained in compliance with HealthData@EU eDelivery specifications and integrated with the ND through a secured SOAP interface.

The operational configuration of the Gateway includes:

- **WS Plugin Setup:** Configured to push SUBMIT_MESSAGE and MESSAGE_STATUS_CHANGE events to the Dispatcher endpoint, as defined in ws-plugin.properties. Retry parameters and timeouts are aligned with eDelivery operational best practices.
- **Endpoint Integration:** The Dispatcher's SOAP endpoint is secured with mutual TLS. The WS Plugin is configured with authentication credentials, retry logic, and the necessary WSDL binding for communication.
- **Certificate and Trust Management:** Domibus is enrolled in the HealthData@EU trust network through certificate-based authentication. Cryptographic materials are securely managed according to national policies. Synchronisation with HealthData@EU trust anchor list and participant metadata is performed periodically.
- **PMode Configuration:** Domibus PMode files are kept aligned with CP specifications, ensuring compatibility in message routing, reliability settings, and security policies. Updates are coordinated by NeHA through formal configuration management.
- **Logging and Observability:** All transport-layer activities are logged locally and integrated, where technically feasible, with the CY-EHDS-2nd observability and audit infrastructure (CPSS4), enabling full traceability and incident resolution.
- **Operational Governance:** All deployment, maintenance, and lifecycle operations are governed by NeHA in alignment with EHDS cross-border communication standards.

4.7 XBDE as the Technical Implementation of National Contact Point Functionalities

The CY-EHDS-2nd WP8 delivers the technical infrastructure that enables Cyprus to act as a fully functional NCP within the HealthData@EU framework. While the term "NCP" refers to a legal and functional role under the EHDS regulation and HealthData@EU governance, WP8 implements all technical enablers required for this role, in alignment with the HealthData@EU CP.

WP8 establishes the XBDE infrastructure, which supports all XBDEs for the secondary use of health data. It enables the reception and transmission of dataset descriptions, data access applications, data permits, and related information in the structured formats and transport protocols defined at EU level.

Specifically, XBDE fulfills key NCP responsibilities by:

- **Establishing the Secure Technical Gateway:** The Domibus-based XBG serves as the secure, AS4-compliant interface for all cross-border communication with the HealthData@EU CP. It is configured according to HealthData@EU trust and transport profiles.
- **Managing Outbound Data Exchange:** The National Dispatcher component manages the preparation, validation, and packaging of national information, such as dataset metadata (from nHDsC) and permit decisions (from DAAMs), into compliant message formats with HealthData@EU. These are securely transmitted to the HealthData@EU CP via the XBG.
- **Processing Inbound Data Exchange:** The National Dispatcher and XBG jointly handle the secure reception of inbound messages, such as data access applications submitted by cross-border data users via the HealthData@EU CP. These messages are validated and routed to the appropriate national systems, such as DAAMs.
- **Ensuring Interoperability and Compliance:** WP8 is implemented in strict alignment with the technical specifications, message formats (e.g. HealthDCAT-AP, JSON schemas), and security protocols (AS4 via eDelivery) defined in HealthData@EU CP Release 3 and the EHDS Regulation. This ensures seamless interoperability with HealthData@EU infrastructure.
- **Facilitating Audited and Traceable Exchanges:** All message exchanges processed by XBDE are logged, timestamped, and made available to the CY-EHDS-2nd observability and audit stack (CPSS4), supporting EHDS requirements for transparency, traceability and accountability.

While the HDAB (NeHA) retains legal and policy-level responsibility for Cyprus role as an NCP, WP8 provides the full technical implementation required to execute XBDE functions in line with EU mandates. The following sections on data flows and requirements further detail how these NCP functionalities are operationalized through XBDE.

4.8 Data Flows

At the heart of cross-border interoperability lies the ability to exchange structured, meaningful, and secure health data across national boundaries. In the context of the EHDS, the XBDE infrastructure operationalizes this vision by orchestrating the continuous flow of information and data between Cyprus and the HealthData@EU CP.

This section describes the bidirectional data flows handled by XBDE, both outbound transmissions from national systems (e.g. datasets and permits), and inbound messages received from the HealthData@EU CP (e.g. data access applications).

4.9 Outbound Data Flows

The XBDE infrastructure handles outbound cross-border communication by securely transmitting structured messages from national systems (DAAMs, nHDsC) to the HealthData@EU CP via AS4/eDelivery. These messages conform to the formats and exchange protocols defined in HealthData@EU CP.

Table 1 summarizes all currently defined outbound flows, indicating which of them will be implemented in the scope of CY-EHDS-2nd.

Table 1: Outbound Cross-Border Data Flows from Cyprus to HealthData@EU CP

No.	Flow Type	Payload Format	Protocol	Responsible Source System	Implemented in CY-EHDS-2nd
1	Dataset Creation	RDF (HealthDCAT-AP)	AS4 via Domibus	nHDsC (WP6)	Yes
2	Dataset Update	RDF (HealthDCAT-AP)	AS4 via Domibus	nHDsC (WP6)	Yes
3	Dataset Deletion	RDF (HealthDCAT-AP)	AS4 via Domibus	nHDsC (WP6)	Yes
4	Data Permit / Data Request	JSON	AS4 via Domibus	DAAMs (WP5)	Yes
5	Permit Lifecycle Update (revoked, expired)	JSON	AS4 via Domibus	DAAMs (WP5)	Supported by internal system design. Awaiting EU interface specification.
6	Data Access Application Status Updates	JSON	AS4 via Domibus	DAAMs (WP5)	Supported by internal system design. Awaiting EU interface specification.
7	SPE Description Metadata	JSON / TBD	AS4 via Domibus	SPE Management (WP7)	No (Acknowledged as future need)
8	Penalties Info	JSON / TBD	AS4 via Domibus	TBD (Future Components)	No (Acknowledged as future need)
9	Transparency Info	JSON / TBD	AS4 via Domibus	TBD (Future Components)	No (Acknowledged as future need)

Outbound flows are triggered by authorized users or system events in the national modules. These actions initiate calls to the National Dispatcher via secure internal APIs. The Dispatcher performs validation and transformation of the payload, generates an AS4 message, and submits it to the XBG (Domibus) for transmission to the HealthData@EU CP.

Only the message types supported by the HealthData@EU CP R3 are implemented within the CY-EHDS-2nd scope. However, the XBDE architecture is designed to accommodate additional flows in future phases once official EU specifications are published.

4.9.1 Outbound Flow: Dataset Catalogue Synchronization to HealthData@EU CP

The Dataset Catalogue Synchronization flow group enables the nHDsC to transmit structured dataset metadata to the HealthData@EU CP, allowing cross-border data users to discover and assess available

datasets for secondary use. This group covers the creation, update, and deletion of dataset records, all processed through a unified technical mechanism (Table 2).

Synchronization operations

Each synchronization message includes an RDF payload describing a dataset according to the HealthDCAT-AP semantic model. The supported operations are:

- create: New dataset is made discoverable via the HealthData@EU CP
- update: Existing dataset metadata is modified
- delete: Dataset description is removed from the HealthData@EU catalogue

Actors

Table 2: Dataset Catalogue Synchronization to HealthData@EU CP Actors as defined in *D5.1 Annex D: Common Actor Definitions – CY-EHDS-2nd (v1.0)*

Actor No.	Actor	Role
A7	nHDsC Manager	Initiates sync by triggering export
A8	nHDsC Auditor	Approves dataset metadata before sync
A14	HealthData@EU CP	Receives and publishes the dataset
A16	nHDsC	Exports RDF record and initiates call to Dispatcher
A19	National Dispatcher	Validates, packages, and transmits message
A20	Domibus Gateway	Sends message to CP

Source and Trigger

The process is manually initiated by the HDAB nHDsC Manager after a dataset record has been created or updated in the national catalogue and approved by the HDAB nHDsC Auditor. Once the manager chooses to synchronize the dataset, the nHDsC system (WP6) exports the dataset record in RDF format and calls the National Dispatcher API to begin the transmission.

Transmission Process

1. nHDsC exports the dataset in RDF (HealthDCAT-AP) format, including metadata such as dataset ID, description, keywords, publisher, access conditions and associated contact point.
2. The National Dispatcher validates the RDF structure and metadata.
3. Based on the operation type (create, update, delete), the Dispatcher wraps the payload in a base64-encoded AS4 message and forwards it to the Domibus-based XBG.
4. Domibus transmits the AS4 message securely to the Central Domibus of the HealthData@EU CP.
5. The message is routed to the CP Catalogue component and becomes accessible to cross-border users via the Union Catalogue portal.

EHDS and HealthData@EU Compliance

- Payload format: RDF in HealthDCAT-AP
- Transmission: AS4 over eDelivery, per HealthData@EU CP R3 specification

4.9.2 Outbound Flow: Data Permit Issuance

This flow enables the secure transmission of a data permit or data request from Cyprus to the HealthData@EU CP, following the approval of a cross-border data access application by the HDAB. Once a data permit or request is issued at national level, it must be synchronized with the HealthData@EU CP.

Synchronization operations

The transmitted payload is a structured permit (or data request), encoded in JSON. It is expected to contain:

- Reference to the originating application or request
- Approved dataset(s) and conditions of use
- Data permit metadata

CY-EHDS-2nd will implement this flow provided that the complete and final structure of the permit payload is made available in time by the HealthData@EU CP.

Actors

The actors involved in the Data Permit Issuance outbound flow are presented in Table 3 as defined in D5.1 Annex D: Common Actor Definitions – CY-EHDS-2nd (v1.0).

Table 3: Data Permit Issuance Actors as defined in D5.1 Annex D: Common Actor Definitions – CY-EHDS-2nd (v1.0)

Actor No.	Actor	Role
A4	Application Manager	Approves cross-border application and initiates permit issuance
A14	HealthData@EU CP	Makes permit available to the original data user
A15	DAAMs	Creates permit JSON and submits to Dispatcher
A19	National Dispatcher	Validates and transmits message
A20	Domibus Gateway	Delivers message to HD@EU CP

Source and Trigger

The trigger is a decision to approve a cross-border application or request, made by the HDAB Application Manager and formalized through the national DAAMs system. Once the permit is approved, DAAMs prepares the payload and initiates the outbound flow.

Transmission Process

1. DAAMs (WP5) generates the JSON permit.
2. The payload is submitted to the National Dispatcher via internal API.
3. The Dispatcher validates and packages the permit in an AS4 message.
4. The AS4 message is submitted to the Domibus XBG.
5. The message is securely delivered to the HealthData@EU CP via Central Domibus.
6. The HealthData@EU CP makes the permit available to the original data applicant.

EHDS and HealthData@EU Compliance

- Message format: JSON
- Protocol: AS4 over eDelivery

4.9.2.1 Outbound Flows: Future

CY-EHDS-2nd focuses on implementing the flows that are technically supported by the HealthData@EU CP R3 but the architecture of XBDE is designed to support additional cross-border message types as soon as formal EU-level specifications become available.

This section describes the outbound flows that are not implemented in this phase, but for which the CY-EHDS-2nd infrastructure has been designed and prepared. These flows are recognized by the EHDS Regulation and HealthData@EU documentation [1-7] as part of the broader functional scope for HDABs [9].

Table 4: Future Outbound Flows

No.	Flow Type	Payload Format	Protocol	Responsible Source System	Included in CY-EHDS-2nd
1	Permit Lifecycle Update (e.g. revoked, expired)	JSON	Not yet defined	DAAMs (WP5)	Supported by internal system design. Awaiting EU interface specification.
2	Data Access Application Status Updates	JSON	Not yet defined	DAAMs (WP5)	Supported by internal system design. Awaiting EU interface specification.
3	SPE Description Metadata	JSON	Not yet defined	HDAB (NeHA)	No (Acknowledged as future need)
4	Penalties Info	JSON	Not yet defined	HDAB (NeHA)	No (Acknowledged as future need)
5	Transparency Info	JSON / PDF	Not yet defined	HDAB (NeHA)	No (Acknowledged as future need)

These flows are currently out of scope for technical implementation in CY-EHDS-2nd due to the absence of:

- Finalized data models or payload schemas
- Agreed transmission protocols
- Platform-side support from HealthData@EU CP

Nevertheless, the XBDE infrastructure is being developed with modularity and forward compatibility in mind. Where applicable, internal events and APIs are already in place to support these future flows with minimal architectural change once EU-level definitions are available (Table 4).

4.10 Inbound Data Flows

Inbound data flows are the entry point of the cross-border interaction between the HealthData@EU CP and the national infrastructure of Cyprus. These messages originate from cross-border data users and are transmitted to Cyprus through the secure AS4-based eDelivery network. Upon receipt, they are processed

by the XBDE National Dispatcher and routed to the appropriate national systems for validation, review, and response.

Only message types formally supported in HealthData@EU CP Release 3 are implemented under CY-EHDS-2nd. However, the XBDE architecture is designed to support additional flows as soon as technical specifications and formats become available from the CP.

Each inbound flow triggers a validated reception process. Messages are processed asynchronously and traced at every stage of receipt, validation, and delivery to internal modules. The XBDE event logging and security model is integrated with the CY-EHDS-2nd CPL services.

Error! Reference source not found. presents the group of inbound flows that are supported in HealthData@EU CP R3 and will be implemented in the CY-EHDS-2nd infrastructure.

Table 5: Inbound Cross-Border Data Flows from HealthData@EU CP to Cyprus

No.	Flow Type	Payload Format	Protocol	Responsible Recipient System	Implemented in CY-EHDS-2nd
1	New or Amended Application Submission	JSON (base64)	AS4 via Domibus	DAAMs (WP5)	Yes

4.10.1 *Inbound Flow: Reception of New or Amended Data Access Applications from HealthData@EU CP*

This inbound flow enables Cyprus to receive structured new and amended data access applications from cross-border data users via the HealthData@EU CP. These submissions are delivered through the HealthData@EU eDelivery infrastructure and represent the official initiation (or re-initiation) of the secondary use access lifecycle.

Amended applications follow the same technical path as initial applications. They are distinguished by referencing a previously submitted application within the payload content and are treated by the receiving system (DAAMs) as a continuation or correction of an existing case.

Reception operations

Each message contains a JSON payload structured according to HealthData@EU schemas, including:

- Applicant information (name, organization, contact)
- Purpose of processing
- Referenced dataset(s)
- Justification of public interest or legal basis
- Attachments (e.g. ethics approval, study protocol)
- (For amendments) a reference to the original application ID

Actors

Table 6: Reception of Data Access Applications from HealthData@EU CP Flow Actors as defined in D5.1
Annex D: Common Actor Definitions – CY-EHDS-2nd (v1.0)

Actor No.	Actor	Role
A2	Data User	Submits the application or request via the Union Portal
A4	Application Manager	Coordinates evaluation of the submission and issues a decision
A14	HealthData@EU CP	Validates and forwards the JSON message via AS4
A15	DAAMs	Receives the structured application/request for processing by HDAB
A19	National Dispatcher	Validates payload, logs transmission, and routes the message
A20	Domibus Gateway	Receives and processes the AS4 message
-	Central Domibus	Transports the message to Cyprus via eDelivery

Source and Trigger

This flow is triggered when a data user in another Member State submits a new or amended application via the HealthData@EU CP. The application is routed through the HealthData@EU CP to Cyprus (**Table 6**).

Reception Process

- HealthData@EU CP sends the AS4 message to the Central Domibus.
- The message is delivered to Cyprus National Domibus via eDelivery.
- The Domibus Gateway receives and passes the message to the National Dispatcher using the WS Plugin (SUBMIT_MESSAGE).
- The Dispatcher validates and logs the payload.
- The application or request is forwarded via internal API to DAAMs (WP5) for further evaluation by the HDAB Application Manager

EHDS and HealthData@EU Compliance

- Protocol: AS4 over eDelivery
- Payload format: JSON, in line with Release 3 specifications

5 REQUIREMENTS AND SPECIFICATIONS

5.1 Functional Requirements

The Functional Requirements (FRs) for XBDE infrastructure responsible are presented in this section targeting a secure, reliable, and compliant cross-border exchange of secondary use health data between the CY-EHDS-2nd national systems and the HealthData@EU CP. These requirements align with the EHDS regulation and the HealthData@EU CP R 3 specifications.

XBDE functionality is strictly defined by EU-level architecture and protocols, and unlike other modules in CY-EHDS-2nd, does not expose a user-facing interface or support optional national workflows. Instead, its role is prescriptive and narrowly scoped: it must process, transform, and transmit information exactly as required

by the HealthData@EU infrastructure. Accordingly, the FRs in this chapter are organized by the two-core technical sub-components of XBDE:

- The ND, responsible for internal API integration, payload transformation, validation, routing, and message tracking
- The Domibus-based XBG, responsible for AS4-based message transport, reception, and delivery acknowledgment via the eDelivery network

Each requirement includes a unique identifier, title, and description. The data flow use cases and detailed inter-component interactions have already been covered in Chapter 4.

5.2 General Cross-Border Requirements

Table 7: General Cross Border FRs

Code	XBDE-FR1
Name	Bidirectional Message Exchange Capability
Description	XBDE must be capable of facilitating both outbound message transmission (from CY-EHDS-2nd to HealthData@EU CP) and inbound message reception (from HealthData@EU CP to CY-EHDS-2nd) using the mandated eDelivery AS4 protocol via XBG (Domibus).
Code	XBDE-FR2
Name	Adherence to HealthData@EU CP Protocols and Formats
Description	XBDE must process, transform (where necessary), and exchange all supported cross-border data types in strict accordance with the data formats (e.g. HealthDCAT-AP RDF, specified JSON schemas), messaging protocols (AS4), and technical interface specifications defined by the HealthData@EU CP R3. Support for additional flows will be enabled once official specifications are published by the EU.
Code	XBDE-FR3
Name	Secure Communication Channel
Description	All external communications handled by WP8 with the HealthData@EU CP (via the XBG) MUST utilize secure channels, employing strong encryption, mutual authentication, and message integrity mechanisms as specified by the eDelivery AS4 profile and HealthData@EU network security policies.
Code	XBDE-FR4
Name	Transaction Traceability and Audit Logging

Description	XBDE must ensure that all significant events in cross-border message exchanges are logged including both transport-level logs (from Domibus) and processing level logs (from the Dispatcher). These logs must be streamed to the CY-EHDS-2nd observability stack (via CPSS4) and available for inspection by authorized HDAB personnel.
-------------	---

5.3 National HealthData@EU Dispatcher Requirements

The ND is the central orchestration sub-component of XBDE. It is responsible for managing all cross-border message preparation, processing, and internal integration tasks on behalf of the CY-EHDS-2nd infrastructure. This includes receiving synchronisation triggers from national systems (e.g. nHDsC and DAAMs), retrieving data payloads, transforming and validating these payloads against EU specifications, constructing AS4 messages, and interacting with the Domibus-based XBG.

On the inbound side, the Dispatcher handles business payloads received via AS4 from the HealthData@EU CP, performs validation, and routes them to the correct national module (e.g. DAAMs). It also manages transaction status updates, error handling, logging, and audit trail generation in line with CPSS4 requirements.

The FRs in Table 8 reflect the precise responsibilities of the ND as implemented under CY-EHDS-2nd, fully aligned with the HealthData@EU CP R3 architecture and message specifications.

Table 8: ND FRs

Code	ND-FR1
Name	Reception of Internal Sync Triggers
Description	The ND must be capable of receiving internal synchronization triggers from national functional modules (e.g. nHDsC, DAAMs). These triggers will indicate that specific national information requires processing for cross-border exchange and must include necessary identifiers (e.g. dataset ID, application ID) and action type.
Code	ND-FR2
Name	Retrieval of Full Data Payloads from National Modules
Description	Upon receiving a synchronization trigger, the ND must securely retrieve the complete and current data payload (e.g. HealthDCAT-AP RDF metadata from nHDsC, JSON application/permit status from DAAMs) from the relevant national source module via its exposed internal API.
Code	ND-FR3
Name	Transformation and Validation of Outbound Data
Description	The ND must validate and transform fetched national data into the precise formats mandated by HealthData@EU CP and EHDS technical specifications for outbound messages. This includes HealthDCAT-AP RDF for dataset metadata and specified JSON structures for applications.
Code	ND-FR4
Name	AS4 Message Construction for Outbound Communication
Description	The National Dispatcher MUST construct well-formed AS4 messages for all outbound communications to the HealthData@EU CP, including appropriate AS4 headers (e.g.

	sender/receiver identifiers, message properties, service/action) and the packaged data payload, adhering to HealthData@EU eDelivery network profiles.
Code	ND-FR5
Name	Submission of Outbound AS4 Messages to XBG
Description	The ND must securely submit all constructed outbound AS4 messages to the national XBG (Domibus) for transmission to the HealthData@EU Central Domibus.
Code	ND-FR6
Name	Reception of Inbound Payloads from XBG
Description	The ND must be capable of receiving inbound business payloads (e.g. EU data access applications/requests, queries, notifications) from the national XBG (Domibus) after AS4-level processing by the gateway.
Code	ND-FR7
Name	Parsing and Validation of Inbound Payloads
Description	For inbound payloads, the ND must parse the data (e.g. JSON application forms) and perform initial validation of structure and content against HealthData@EU CP specifications and expected formats.
Code	ND-FR8
Name	Notification to National Modules for Inbound Data
Description	After successfully processing an inbound payload, the ND must notify the appropriate target national module (e.g. DAAMs for new EU applications) by publishing a clearly defined event to the shared CY-EHDS-2nd event bus. This event must facilitate the retrieval or include the data for national processing.
Code	ND-FR9
Name	AS4 Transaction Status Management
Description	The ND must process AS4-level acknowledgments (e.g. RECEIPT, ERROR signals) received from the XBG related to outbound messages and update the status of the corresponding cross-border transaction accordingly.
Code	ND-FR10
Name	Error Handling and Retry Logic for Dispatch
Description	The ND must implement robust error handling for its operations. This includes configurable retry mechanisms for transient failures in communication with national modules or the XBG, and escalation of non-recoverable errors (e.g. via event publication to the Monitoring/Alerting System).
Code	ND-FR11
Name	Internal API Provision and Consumption
Description	The ND must expose secure internal APIs for national modules to trigger synchronisation processes. It must also securely consume APIs exposed by nHDsC and DAAMs for data payload retrieval. All such APIs MUST adhere to OpenAPI 3.0 standards and CY-EHDS-2nd security policies.

5.4 Cross-Border Gateway (Domibus) Requirements

The XBG sub-component of XBDE is implemented using Domibus, the EC open-source reference implementation of an eDelivery AS4 Access Point. Its primary function is to provide secure, reliable, and policy-compliant transport of AS4 messages between the CY-EHDS-2nd ND and the HealthData@EU CP, using the configurations and security profiles defined in the HealthData@EU eDelivery network.

The following FRs in Table 9 apply specifically to the configuration and operation of the Domibus instance within XBDE. This includes AS4 message exchange, acknowledgment handling, security enforcement, and transaction-level logging. Peer-to-peer NCP communication is not supported in the HealthData@EU CP architecture and is therefore not part of CY-EHDS-2nd.

Table 9: XBG Functional Requirements

Code	XBG-FR1
Name	AS4 Message Transmission (Outbound)
Description	The XBG (Domibus) must securely transmit AS4 messages, received from the CY-EHDS-2nd ND to the designated recipient Access Point (e.g. HealthData@EU Central Domibus) in compliance with the HealthData@EU eDelivery network AS4 profile and configured PModes.
Code	XBG-FR2
Name	AS4 Message Reception (Inbound)
Description	The XBG (Domibus) must securely receive AS4 messages from the HealthData@EU Central Domibus, performing necessary AS4-level processing (e.g. decryption, signature verification) according to the established PMode configurations.
Code	XBG-FR3
Name	Payload Delivery to National Dispatcher (Inbound)
Description	Upon successful reception and AS4-level processing of an inbound message, the XBG (Domibus) must make the extracted business payload available to the WP8 ND, typically via a configured Domibus plugin (e.g. WS-Plugin) or other standard Domibus backend interface.
Code	XBG-FR4
Name	AS4 Acknowledgment Handling
Description	The XBG (Domibus) must automatically generate and send AS4-level acknowledgments (e.g. RECEIPT signals) for received messages, and process acknowledgments received for outbound messages, according to the AS4 standard and configured PModes. These acknowledgment statuses MUST be made available to the National Dispatcher.
Code	XBDE-FR5
Name	AS4 PMode Configuration and Compliance
Description	The XBG (Domibus) must be configured with PModes that are fully compliant and aligned with the PMode specifications provided or mandated by the HealthData@EU CP operators for communication within the HealthData@EU eDelivery network.

Code	XBDE-FR6
Name	AS4 Message Security (Signing and Encryption)
Description	The XBG (Domibus) must apply AS4 message-level security, including digital signing of outbound messages and decryption of inbound messages, using HDAB (NeHA) managed certificates and algorithms compliant with the HealthData@EU eDelivery network security requirements. Payload encryption must be supported as per the AS4 profile.
Code	XBDE-FR7
Name	Non-Repudiation Support
Description	Through its AS4 protocol implementation, the XBG (Domibus) must support NRO for sent messages and NRR for received messages, as defined by the eDelivery AS4 standard and required by the HealthData@EU network.
Code	XBDE-FR8
Name	Domibus Transaction Logging
Description	The XBG (Domibus) must generate detailed logs for all AS4-level transport activities (e.g. message submission, reception, acknowledgments, errors, security processing). These logs must be integrated with the CY-EHDS-2nd shared observability stack for audit and troubleshooting purposes.

5.5 Non-functional Requirements

The NFRs for XBDE define the quality attributes, operational capabilities, and compliance obligations necessary for the reliable, secure, and legally compliant functioning of the XBDE infrastructure. As XBDE enables Cyprus to act as the NCP in the HealthData@EU network, its performance must satisfy both technical standards and legal frameworks including the EHDS Regulation and GDPR. The NFRs are categorized for clarity and address key aspects relevant to the component XBDE under six categories outlined in Table 10.

Table 10: Overview of the NFRs Categories of XBDE

No.	NFRs Category	Purpose
WP8NFR1	Performance Efficiency	Ensures responsiveness, processing speed and scalability of XBDE components.
WP8NFR2	Interoperability	Ensures compliance with data formats, standards and protocols used in HealthData@EU CP.
WP8NFR3	Reliability	Ensures continuous operation, resilience and recoverability of cross-border message flows.
WP8NFR4	Security	Protects all cross-border communication and internal message handling against threats.
WP8NFR5	Maintainability	Supports ease of updates, configurability, diagnosability and testing.
WP8NFR6	Compliance	Ensures full adherence to legal, regulatory and HealthData@EU technical specifications.

5.6 WP8NFR1 - Performance Efficiency

The Performance Efficiency NFRs for XBDE address the system's responsiveness, resource consumption, and ability to handle its workload effectively in the context of XBDE in Table 11. While the anticipated initial

volume of transactions for CY-EHDS-2nd may be low, XBDE must be designed to perform efficiently and be capable of scaling to accommodate potential future growth in cross-border interactions within the HealthData@EU network. These NFRs ensure that XBDE does not become a bottleneck and can process messages in a timely manner.

Table 11: WP8 - NFR - Performance Efficiency

Category	WP8NFRC1 - Performance Efficiency
Code	WP8-NFR1
Name	Internal Trigger Processing Latency
Description	The ND must process internal synchronization triggers received from national modules (e.g. nHDsC, DAAMs) within a defined timeframe under normal conditions.
Measure / Compliance Indicator	- 95th percentile of event processing and trigger dispatch time < X seconds (Value X to be defined post-benchmarking).
Code	WP8-NFR2
Name	Outbound Processing Time
Description	Upon receiving a trigger, the ND must complete fetching, transformation, and message construction within a defined timeframe.
Measure / Compliance Indicator	- 95th percentile of internal processing time for outbound messages < Y seconds (Value Y to be defined post-benchmarking).
Code	WP8-NFR3
Name	Inbound Processing Time
Description	After receiving an inbound payload from Domibus, the ND must complete parsing, validation, and event notification to national modules within Z seconds.
Measure / Compliance Indicator	- 95th percentile of internal processing time for inbound messages < Z seconds (Value Z to be defined post-benchmarking).
Code	WP8-NFR4
Name	Domibus Throughput
Description	The XBDE (Domibus) MUST handle peak AS4 message load without queue overload or degradation.
Measure / Compliance Indicator	- System capable of processing A messages per hour (Value A to be estimated based on projected peak load and confirmed via load testing) with internal Domibus queue lengths remaining below defined thresholds.
Code	WP8-NFR5
Name	Resource Utilization
Description	ND and Domibus must operate under defined resource thresholds.
Measure / Compliance Indicator	- CPU utilization < 70% average - Memory utilization < 80% average under defined peak load conditions for sustained periods (specific thresholds to be set by NeHA). - Monitored via observability platform.
Code	WP8-NFR6

Name	Scalability
Description	The ND must be designed to be horizontally scalable where technically feasible. The system should allow for an increase in processing capacity by adding more instances of these components to handle potential future growth in cross-border message volume without requiring significant architectural redesign.
Measure / Compliance Indicator	- Demonstration via deployment configuration that key components (National Dispatcher) can be scaled by increasing replica counts.

5.7 WP8NFRC2 - Interoperability

Interoperability is a cornerstone NFR for XBDE, as its primary purpose is to enable seamless and compliant data exchange between the CY-EHDS-2nd national infrastructure and the HealthData@EU CP, as well as with other national systems within Cyprus. Table 12 define the requirements that ensure XBDE can effectively communicate and exchange data using agreed-upon standards, protocols and data formats.

Table 12: NFR - Interoperability

Category	WP8NFRC2 - Interoperability
Code	WP8-NFR7
Name	AS4 Protocol Compliance for XBG
Description	The XBG (Domibus) must strictly adhere to the eDelivery AS4 profile and related technical specifications (including security policies and PMode configurations) mandated by the HealthData@EU CP for all communications within the HealthData@EU network.
Measure / Compliance Indicator	- Successful completion of HealthData@EU conformance testing for AS4 communication. - Demonstrated ability to exchange AS4 messages (send/receive and process acknowledgments) with the HealthData@EU Central Domibus test environment and subsequently production. - PMode configurations verified against HealthData@EU CP specifications.
Code	WP8-NFR8
Name	HealthDCAT-AP Compliance for Outbound Metadata
Description	All dataset metadata prepared by the ND for outbound transmission to the HealthData@EU CP must be fully compliant with the latest adopted version of the HealthDCAT-AP standard, as specified by HealthData@EU CP and relevant EHDS Implementing Acts.
Measure / Compliance Indicator	- Successful validation of generated RDF/ eXtensible Markup Language (XML) metadata against the official HealthDCAT-AP SHACL shapes and any additional validation rules specified by HealthData@EU CP. - Successful ingestion of submitted metadata by the HealthData@EU CP test/production environment.
Code	WP8-NFR9
Name	Standardized JSON Format Compliance for Applications and Statuses
Description	All data access application forms and data permit/data request information exchanged by XBDE with the HealthData@EU CP (both outbound and inbound) MUST adhere to the standardized JSON schemas and structures defined by HealthData@EU CP R3 and subsequent binding EHDS Implementing Acts.

Measure / Compliance Indicator	- Successful validation of generated/received JSON payloads against the official JSON schemas provided by HealthData@EU CP. - Successful processing of these JSON messages by both the CY-EHDS-2nd National Dispatcher (for inbound) and the HealthData@EU CP Data Access component (for outbound).
Code	WP8-NFR10
Name	Internal API Interoperability (OpenAPI)
Description	All internal APIs exposed or consumed by XBDE sub-components (e.g. between ND and nHDsC or DAAMs) must be documented using OpenAPI 3.0 specification and adhere to RESTful design principles, ensuring clear, standardized, and discoverable interfaces within the CY-EHDS-2nd infrastructure.
Measure / Compliance Indicator	- Availability of valid OpenAPI 3.0 specification documents for all defined internal APIs. - Successful integration testing between XBDE sub-components and with other national modules (nHDsC, DAAMs) based on these API specifications.

5.8 WP8NFR3 - Reliability

The Reliability NFRs for WP8 define the system's ability to perform its required functions under stated conditions for a specified period. Given XBDE critical role as the national gateway for cross-border health data exchange, high reliability is essential to ensure consistent service, prevent data loss and maintain trust in the CY-EHDS-2nd infrastructure and its participation in the HealthData@EU network. This section covers aspects such as service maturity, availability, fault tolerance and recoverability (Table 13).

Table 13: NFR – Reliability

Category	WP8NFR3 -Reliability
Code	WP8-NFR12
Name	Maturity of Core Transport Technology (Domibus)
Description	The XBG sub-component of XBDE must be implemented using Domibus, which is the EU-endorsed, mature, and widely adopted open-source sample implementation of an eDelivery AS4 Access Point. This leverages a proven technology stack for core message transport reliability.
Measure / Compliance Indicator	- Confirmation of Domibus version used and its status as a stable, supported release. - Adherence to Domibus configuration best practices as recommended by the EC and the HealthData@EU operational team.
Code	WP8-NFR13
Name	WP8 Service Availability
Description	All critical XBDE services (XBG, National Dispatcher) must achieve a high level of availability (e.g. 99.9% monthly uptime) during defined service hours, minimizing unplanned downtime for cross-border communication capabilities. Scheduled maintenance windows must be pre-announced and minimized.
Measure / Compliance Indicator	- Monthly availability percentage calculated based on monitoring data (Target: ≥99.9% or as defined by NeHA Service Level Agreement (SLA)). - Duration and frequency of unplanned outages. Adherence to scheduled maintenance protocols.
Code	WP8-NFR14
Name	Fault Tolerance of WP8 Components

Description	XBDE components must be designed for fault tolerance. Failure of a single instance of a scalable component (e.g. National Dispatcher) must not lead to a complete loss of XBDE functionality. The system should leverage underlying platform capabilities (e.g. Kubernetes) for automatic restart and rescheduling of failed component instances.
Measure / Compliance Indicator	- Successful failover testing demonstrating continued service (possibly with graceful degradation) upon simulated failure of one or more component instances (within defined redundancy limits). - Monitoring alerts for component failures and successful automated recovery.
Code	WP8-NFR15
Name	eDelivery AS4 Message Reliability
Description	XBDE, through its XBG (Domibus), must leverage the inherent reliability mechanisms of the AS4 protocol, including guaranteed message delivery, duplicate detection, and message ordering (where specified by PModes), for all communications within the HealthData@EU network.
Measure / Compliance Indicator	- Domibus logs demonstrating successful use of AS4 reliability features (e.g. acknowledgments, error signals). - Successful completion of eDelivery conformance tests that verify reliable messaging. Low rate of undelivered or lost messages in test and production environments.
Code	WP8-NFR16
Name	Data Persistence and Recoverability for Transactions
Description	The ND must ensure that the state and essential metadata of all in-flight and completed cross-border transactions (both inbound and outbound) are persisted reliably. In the event of a component failure, the system must be able to recover to a consistent state and resume or correctly finalize processing of these transactions.
Measure / Compliance Indicator	- Defined backup and recovery procedures for XBDE persistent data (e.g. transaction state database for the Dispatcher). - Successful execution of disaster recovery drills demonstrating restoration of XBDE services and transaction states within a defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO) set by NeHA.
Code	WP8-NFR17
Name	Graceful Degradation
Description	In the event of partial system failures or high load conditions impacting dependent national modules (e.g. nHDsC, DAAMs) XBDE must degrade gracefully. It should prioritize critical functions (e.g. receiving inbound messages) and queue or manage less critical tasks (e.g. some outbound triggers) appropriately, providing informative error messages or status where possible.
Measure / Compliance Indicator	- System behavior observed during stress tests and fault injection tests. - Monitoring of error rates and queued tasks under adverse conditions. - Continued operation of core inbound message reception during simulated partial outages of connected national systems.

5.9 WP8NFR4 – Security

Security is a paramount NFR for WP8, given its role in handling potentially sensitive (though typically metadata or status, not raw health data) information and acting as the official gateway for cross-border health data related exchanges. XBDE must implement robust security measures at all levels including application, data and transport, to protect against unauthorized access, modification, disclosure, or denial of service, ensuring compliance with the EHDS Regulation, GDPR, HealthData@EU CP security policies, and national security mandates (Table 14).

Table 14: NFR – Security

Category	WP8NFR4 – Security
Code	WP8-NFR18
Name	Secure Transport Layer (AS4)
Description	All cross-border communications facilitated by the XBG (Domibus) with the HealthData@EU CP network must use the AS4 protocol configured with strong encryption (e.g. TLS for the underlying transport, AS4-level payload encryption where specified by PMode) and mutual authentication using digital certificates, adhering to HealthData@EU eDelivery security profiles.
Measure / Compliance Indicator	- Verification of Domibus configuration against HealthData@EU security specifications. - Successful AS4 exchanges using mandated encryption and authentication mechanisms during conformance and interoperability testing. - Penetration testing results validating TLS.
Code	WP8-NFR19
Name	Message Integrity and Authenticity (AS4)
Description	The XBG (Domibus) must ensure the integrity of exchanged AS4 messages through digital signatures and verify the authenticity of received messages using digital certificates, as per the AS4 standard and HealthData@EU PMode configurations.
Measure / Compliance Indicator	- Domibus logs and successful message exchanges demonstrating correct application and verification of digital signatures. - Test cases validating rejection of messages with invalid or tampered signatures.
Code	WP8-NFR20
Name	NRO & NRR (AS4)
Description	WP8, through its XBG (Domibus), must support AS4 mechanisms for NRO for sent messages and NRR for received messages, ensuring legally binding proof of exchange as required by the HealthData@EU network.
Measure / Compliance Indicator	- Successful generation and processing of AS4 RECEIPT signals incorporating non-repudiation information. - Conformance with eDelivery specifications for non-repudiation evidence.
Code	WP8-NFR21
Name	Secure Internal WP8 Communication
Description	All internal communication between XBDE sub-components (e.g. National Dispatcher to local Domibus interfaces) must occur over secure channels (e.g. mTLS within the Kubernetes cluster) and employ appropriate authentication and authorization mechanisms to prevent unauthorized internal access or data interception.
Measure / Compliance Indicator	- Network configuration review confirming secure protocols for internal traffic. - Successful internal API calls requiring authentication/authorization. - Penetration testing including assessment of internal communication security.
Code	WP8-NFR22
Name	Access Control for XBDE APIs and Configuration
Description	Access to any administrative or internal APIs exposed by XBDE components, as well as access to XBDE configuration settings (including Domibus PModes and security certificates), must be strictly controlled through strong authentication and role-based authorization mechanisms managed by the HDAB (NeHA). Only authorized NeHA personnel should have access.

Measure / Compliance Indicator	- RBAC policies defined and enforced for WP8 APIs and configuration interfaces. - Audit logs demonstrating access attempts and enforcement of permissions. - Regular review of access rights.
Code	WP8-NFR23
Name	Protection of Sensitive Configuration Data
Description	All sensitive configuration data used by XBDE, particularly Domibus PModes, private keys, certificates, and API keys for internal communication, must be stored securely (e.g. using encrypted secrets management solutions provided by the hosting platform) and protected against unauthorized access or disclosure.
Measure / Compliance Indicator	- Use of approved secrets management tools. - Regular security audits of configuration storage. - Evidence of encryption at rest for sensitive configuration items.
Code	WP8-NFR24
Name	Vulnerability Management for XBDE Components
Description	XBDE components, including the Domibus instance and any custom-developed software (i.e. National Dispatcher), must undergo regular vulnerability scanning and patching. A process must be in place for timely remediation of identified vulnerabilities according to their severity, as defined by HDAB (NeHA) security policy.
Measure / Compliance Indicator	- Regular vulnerability scan reports. - Patch management policy and records demonstrating timely application of security updates. - Evidence of remediation for critical/high vulnerabilities within defined timeframes.

5.10 WP8NFR5 – Maintainability

The Maintainability NFRs for XBDE address the ease with which the system and its sub-components can be modified, corrected, adapted, and supported throughout its operational lifecycle. Given that XBDE must align with evolving HealthData@EU specifications, national requirements, and potentially new EHDS Implementing Acts, high maintainability is crucial for ensuring long-term viability, cost-effectiveness, and responsiveness to change. This section covers aspects such as modularity, configurability, analyzability (diagnostics), modifiability and testability (Table 15).

Table 15: NFR – Maintainability

Category	WP8NFR5 – Maintainability
Code	WP8-NFR25
Name	Modularity of XBDE Sub-Components
Description	XBDE must be designed with clear modularity between its core sub-components: ND and the XBG (Domibus). Each sub-component should have well-defined responsibilities and interfaces, allowing for independent updates or modifications with minimal impact on other sub-components where feasible.
Measure / Compliance Indicator	- Architectural review confirming clear separation of concerns and defined interfaces (e.g. OpenAPI for internal APIs, event schemas for event bus).

	-Demonstration that an update to one sub-component does not necessitate code changes in an unrelated sub-component (e.g. Domibus AS4 transport logic), provided interfaces remain stable.
Code	WP8-NFR26
Name	Configurability of XBDE Operations
Description	Key operational parameters and business rules within XBDE must be externally configurable rather than hardcoded. This includes, but is not limited to, National Dispatcher data transformation mappings (if any are dynamic), retry policies, logging levels, and Domibus PMode parameters. Configurations MUST be version-controlled and managed by HDAB (NeHA).
Measure / Compliance Indicator	- Identification of key configurable parameters in system documentation. - Demonstration that changes to these parameters can be applied without code recompilation/redeployment of the core application logic. - Version control system used for managing configuration files.
Code	WP8-NFR27
Name	Analyzability and Diagnosability of XBDE Issues
Description	XBDE must provide sufficient logging and monitoring capabilities to allow authorized HDAB (NeHA) technical personnel to effectively analyze system behavior, diagnose issues and troubleshoot failures in cross-border communication. This includes a clear correlation of logs across XBDE sub-components and with Domibus transaction logs.
Measure / Compliance Indicator	- Availability of comprehensive and correlated logs in the shared observability stack. – Successful diagnosis of simulated faults within defined timeframes using available logs and monitoring tools. - Documentation of troubleshooting procedures for common XBDE issues.
Code	WP8-NFR28
Name	Modifiability and Adaptability of XBDE
Description	The architecture and implementation of XBDE must facilitate modifications and adaptations to accommodate future changes in HealthData@EU CP specifications, EHDS Implementing Acts, or national cross-border exchange requirements with reasonable effort and minimal disruption to existing functionalities. This includes adaptability of data transformation and messaging logic.

Measure / Compliance Indicator	- Architectural review assessing amenability to change (e.g. use of design patterns that support extension, clear separation of data mapping logic). - Impact analysis for sample anticipated changes demonstrating localized impact. - Ease of updating to new versions of underlying components (e.g. Domibus, libraries) where security or functionality dictates.
Code	WP8-NFR29
Name	Testability of XBDE Components and Flows
Description	Each XBDE sub-component must be designed to be testable, both in isolation (unit tests) and as part of integrated end-to-end cross-border data flows. Automated testing capabilities should be implemented for core functionalities to support regression testing and continuous integration/continuous deployment (CI/CD) practices.
Measure / Compliance Indicator	- Availability of unit tests for key logic National Dispatcher. - Documented integration test cases covering primary outbound and inbound data flows. - Successful execution of automated regression test suite as part of the CI/CD pipeline. -Ability to simulate interactions with HealthData@EU CP test environments.

5.11 WP8NFR6 – Compliance

The Compliance NFRs for XBDE define the requirements for adherence to all applicable legal, regulatory, and standards-based obligations. As the national gateway for cross-border secondary use of health data related exchanges, XBDE must operate in full conformity with the EHDS regulation and GDPR and the specific technical and operational standards set forth by the HealthData@EU CP. This section underscores the critical importance of legal and regulatory adherence in all aspects of XBDE design and operation (Table 16).

Table 16: NFR – Compliance

Category	WP8NFR6 – Compliance
Code	WP8-NFR30
Name	Adherence to EHDS Regulation for Cross-Border Exchange
Description	XBDE must implement all functionalities and processes related to cross border connection with HD@EU CP (e.g. acting as the NCP, facilitating data flow for applications, metadata, permits) in strict compliance with the relevant articles and provisions of the EHDS Regulation (EU 2025/327).
Measure / Compliance Indicator	- Traceability matrix mapping XBDE functionalities to specific EHDS Regulation articles. -Legal review by HDAB (NeHA) confirming alignment of XBDE design and operational procedures with EHDS mandates for NCPs and XBDE. -Evidence of implementing required safeguards and procedures defined in the Regulation.
Code	WP8-NFR31
Name	GDPR Compliance for Personal Data Handling

Description	Although XBDE primarily handles metadata, application forms, and status information (not typically raw patient health data), any personal data processed by XBDE (e.g. identifiers of data applicants or HDAB personnel in logs or message headers) must be handled in strict compliance with the GDPR, including principles of data minimization, purpose limitation, and security.
Measure / Compliance Indicator	- Data Protection Impact Assessment (DPIA) for XBDE if processing personal data. -Implementation of technical and organizational measures ensuring GDPR compliance (e.g. access controls, audit logs, data retention policies for logs). -Confirmation from HDAB (NeHA) Data Protection Officer (DPO).
Code	WP8-NFR32
Name	Compliance with HealthData@EU CP Specifications
Description	XBDE must maintain ongoing compliance with the latest adopted technical specifications, API definitions, data formats (HealthDCAT-AP, JSON schemas), security profiles, and operational guidelines published by the HealthData@EU CP (currently Release 3 and subsequent updates) for NCPs.
Measure / Compliance Indicator	- Successful participation in HealthData@EU conformance and interoperability testing cycles. - Verification of XBDE configurations (e.g. Domibus PModes, API payloads) against current HealthData@EU CP documentation. - Regular review and update process by HDAB (NeHA) to align with new HealthData@EU CP releases/specifications.
Code	WP8-NFR33
Name	Adherence to National Legal and Policy Framework (Cyprus)
Description	XBDE must operate in accordance with the Cypriot national eHealth law (and its future amendments concerning secondary use of health data) and any specific policies or directives issued by the HDAB (NeHA) regarding the management and operation of the NCP for secondary use.
Measure / Compliance Indicator	- Legal review by HDAB (NeHA) confirming WP8 operational procedures align with national laws and policies. - Configuration of XBDE functionalities reflecting any specific national requirements for XBDE governance.
Code	WP8-NFR34
Name	Auditability for Compliance Verification
Description	XBDE must generate and securely retain comprehensive audit sufficient to enable HDAB (NeHA) and other authorized auditors to verify WP8 compliance with all applicable legal, regulatory, and standards-based obligations.
Measure / Compliance Indicator	- Audit logs containing sufficient detail to reconstruct cross-border transaction histories and system actions. - Successful completion of internal and external audits related to XBDE operations. - Availability of audit log export capabilities in a standard, usable format for auditors.

6 CONCLUSIONS AND NEXT STEPS

XBDE constitutes a critical component of the national infrastructure for the secondary use of health data in the Republic of Cyprus. Its architecture is based on a ND and a Domibus-based eDelivery Gateway and it provides the core capabilities for Cyprus to function as a compliant and interoperable NCP within the EHDS.

XBDE enables Cyprus to exchange data bidirectionally with the HealthData@EU CP, in full alignment with the specifications defined in Release 3. This includes publishing national dataset metadata (via nHDsC) and communicating applications for data permit and data request (via DAAMs). All communications are managed securely using the eDelivery AS4 protocol, and structured using standardized formats including HealthDCAT-AP and JSON schemas as defined by the EC.

The solution has been designed for high interoperability, security, and maintainability, and integrates seamlessly with the other modules developed under the CY-EHDS-2nd initiative. All specifications have been developed in line with the legal framework set by the EHDS Regulation (EU 2025/327) and the GDPR.

The specification outlined in this deliverable reflects a strategic commitment to maximizing reuse of EU components, minimizing divergence from common standards, and enabling the long-term sustainability of Cyprus participation in the EHDS. It provides a complete and actionable blueprint for the design, implementation, and operation of the national cross-border connection.

6.1 Next Steps

The next phase of the CY-EHDS-2nd project is the development and deployment of the national pilot infrastructure. This will bring together all CY-EHDS-2nd module from WP5 through WP9, into an integrated pilot environment. WP8 will be developed and configured as part of this environment, operating with other components to simulate and validate real-world use cases.

The pilot phase will focus on functional implementation and initial validation. This includes deploying the technical infrastructure, testing interoperability with the HealthData@EU CP, and verifying system behavior using live-like scenarios. The goal is to confirm operational readiness, uncover any gaps or limitations, and implement necessary adjustments before moving to production.

While production deployment will follow in a subsequent phase, it is essential that the pilot is executed with sufficient realism to inform that transition. Equally important is establishing the processes and governance structures that will support continuous monitoring and adaptation of WP8 and related components. As the EHDS ecosystem evolves, XBDE must remain adaptable. Updates to the HealthData@EU CP specifications, forthcoming EHDS Implementing Acts, TEHDAS2 implementation guidelines, and amendments to the national eHealth law will all influence the future operation of the system. CY-EHDS-2nd and NeHA as the national HDAB will ensure that WP8 is maintained in alignment with these developments, supporting the long-term role of Cyprus in the EHDS.

7 REFERENCES

1. **European Commission, Directorate-General for Health and Food Safety (2025).** *HealthData@EU CP – 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 CP – 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 EU (2025).** *Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the EHDS 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](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.