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

Proposal number: 101129405

D7.1 SPE: 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
Nicoletta	Prentza	Cyprus	UCY	AE
Waqar Aziz	Sulaiman	Cyprus	UCY	AE
Constantinos	Pattichis	Cyprus	UCY	AE

Reviewed by

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

Abbreviations

2FA	two-factor authentication
ACLs	Access Control Lists
AE	Affiliated Entity
API	Application Programming Interface
CA	Competent Authority
CNIL	French data protection authority
COO	Coordinator
CP	Central Platform
CPL	Central Platform Layer
CY-EHDS-2nd	European Health Data Space for Secondary Use @CY
DAAMs	Data Access Application Management solution
DBCs	Digital Business Capabilities
DGA	Data Governance Act
EC	European Commission
EHDS	European Health Data Space
EHDS2	European Health Data Space for the secondary use of health data
eID	electronic IDentification
ESPE	External Securing Processing Environment
EU	European Union
FRs	Functional Requirements
GDPR	General Data Protection Regulation
GIP	Public Interest Grouping
HDAB	Health Data Access Body
HDH	Health Data Hub
ISPE	Internal Secure Processing Environment
mTLS	mutual Transport Layer Security
NCP	National Contact Point
NeHA	National eHealth Authority of Cyprus
NFRs	Non-Functional Requirements
nHDsC	National Health Dataset Catalogue
RBAC	Role-based access control
SFTP	Secure File Transfer Protocol
SPE	Secure Processing Environment
TEHDAS2	Second Joint Action Towards the European Health Data Space
UCP	Union Contact Point
UCY	University of Cyprus
UDAS	Union Data Access Service
VM	Virtual Machine
WP	Work Package
XBG	Cross-Border Gateway

Executive Summary

The European Health Data Space (EHDS) Regulation (EU) 2025/327[1] mandates that the secondary use of health data be conducted exclusively within Secure Processing Environments (SPEs) that meet stringent privacy and cybersecurity standards. Health Data Access Bodies (HDABs) must ensure that sensitive electronic health data is accessed by authorized users only through such controlled settings, with no personal data leaving them. SPEs are thus a cornerstone for compliant health data reuse, enabling researchers and other authorized users to analyse health datasets under strict safeguards, thereby building trust by protecting patient privacy while facilitating valuable secondary uses of health data (e.g. for research, policy and innovation) in full alignment with EU data protection regulations.

This deliverable, D7.1 'SPE: Requirements and Specifications', is produced under the European Health Data Space for Secondary Use @CY (CY-EHDS-2nd)[2] project, aimed at implementing the EHDS infrastructure and governance in Cyprus. Its purpose is to define the requirements and design specifications for establishing a national SPE in compliance with the EHDS Regulation. The deliverable's scope encompasses identifying the capabilities the SPE must provide, the security and data protection measures it must enforce, and its operational context within the broader EHDS ecosystem.

Given that Cyprus does not currently have a national SPE infrastructure for this purpose, and that the HealthData@EU[3] Central Platform (CP) does not provide a ready-made SPE solution for Member States [1-2], this document details a national Cypriot SPE. The design is guided by best practices and is architected for full compliance with the EHDS Regulation, particularly Article 73.

The CY-EHDS-2nd SPE adopts a two-tier model operated exclusively by the National eHealth Authority of Cyprus (NeHA)[4], which is the national designated HDAB:

- An **Internal Secure Processing Environment (ISPE):** An isolated, secure zone where authorized NeHA operators ingest and prepare raw health datasets from Data Holders (e.g. pseudonymisation, aggregation) according to approved data permits or requests.
- An **External Secure Processing Environment (ESPE):** A separate, secure workspace where approved Health Data Users access the prepared datasets for analysis within a controlled environment using authorized tools, with no direct data export capabilities.

Both environments operate under a unified governance framework managed by NeHA to ensure end-to-end compliance.

Key elements addressed in this deliverable include:

- **SPE Architecture (Internal and External):** A description of the two-tier SPE model, delineating roles and responsibilities (from data providers and HDAB operators to data users) and how these two SPE components interconnect through secure workflows.
- **Functional requirements (FRs) and Non-Functional Requirements (NFRs):** A detailed definition of the SPE requirements, covering functional capabilities (user access management, data ingestion,

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

analysis tools, audit logging, result export controls) and non-functional criteria (performance, availability, security standards, compliance obligations), ensuring adherence to the highest standards mandated by EHDS.

- **Technical Architecture and Specifications:** An outline of the high-level system architecture and technical components, including strong user authentication (integrated with the national electronic IDentification (eID) via the CY-EHDS-2nd Central Platform Layer (CPL)), fine-grained access controls based on data permits (originating from Data Access Application Management solution (DAAMs)), encryption of data, continuous monitoring and mechanisms for reviewed export of non-personal results.

These specifications translate requirements into an actionable design, providing a clear reference for the development and deployment of a pilot SPE in subsequent project phases. The alignment of this SPE design with the EHDS Regulation is explicitly detailed in chapter 855 of this document.

Deliverable D7.1 provides a policy-aligned framework for implementing SPEs in Cyprus, establishing a trusted platform for secure, privacy-preserving and EHDS-compliant health data reuse. It lays the groundwork for a secure, interoperable health data infrastructure that will support researchers, policymakers and other stakeholders, while steadfastly upholding the privacy and rights of individuals. The CY-EHDS-2nd project is committed to the ongoing refinement of these specifications to ensure full alignment with forthcoming EU Implementing Acts for SPEs.

Table of contents

List of Figures

List of Tables

1 INTRODUCTION

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

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

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

To support this shared structure and ensure full coherence across the Work Packages (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 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, National Health Dataset Catalogue (nHDsC), DAAMs, SPE, National Connector and Quality Toolbox, are interconnected through a central coordination layer (the 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 European Union (EU) deliverables,

including outputs from Second Joint Action Towards the European Health Data Space (TEHDAS2), QUANTUM, and the upcoming EHDS implementing acts.

1.1.1.2 Annex B – HDAB Digital Business Capabilities

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

1.1.1.3 Annex C – Indicative Mapping to HealthData@EU Central Platform Infrastructure

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

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

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

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

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

1.1.2 Recommended Reading Order

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

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

6. D7.1 – SPE: Requirements and Specifications
7. D8.1 – National Connector for Cross-border gateway Requirements and Specifications

1.2 D7.1 Introduction

The EHDS, established by Regulation (EU) 2025/327, represents a landmark initiative to empower individuals with greater control over their health data and to foster a vibrant single market for digital health services and products, while enabling the ethical and secure secondary use of health data for research, innovation, policymaking and regulatory activities. A fundamental requirement of the EHDS Regulation for the secondary use of electronic health data is that such processing must occur exclusively within SPEs. These SPEs are mandated to meet stringent technical and organisational measures to ensure the privacy, security and confidentiality of sensitive health information (EHDS Regulation, Article 73).

This deliverable, D7.1 'SPE: Requirements and Specifications', is a key output of the CY-EHDS-2nd which is a project with the primary objective to implement the necessary infrastructure and governance framework for the EHDS in Cyprus. As Cyprus currently does not possess a dedicated national SPE infrastructure for the secondary use of health data and acknowledging that the HealthData@EU CP does not currently provide a ready-made SPE solution for Member States, this document serves to define the comprehensive requirements and foundational specifications for establishing such an environment.

The purpose of this deliverable is to provide a detailed blueprint for the national Cypriot SPE. This includes:

- Outlining the technical architecture and key specifications for its components.
- Describing the operational lifecycle, roles and responsibilities associated with the SPE.
- Defining the FR and NFR for the SPE.
- Ensuring and demonstrating full alignment with the EHDS Regulation, particularly Article 73.

The proposed national Cypriot SPE adopts a two-tier model, operated and governed by NeHA in its capacity as the designated HDAB for Cyprus:

- An **ISPE:** An isolated environment for authorized NeHA personnel to securely ingest, prepare and manage health datasets according to approved data permits or requests.
- An **ESPE:** A controlled and isolated workspace provisioned for authorized Health Data Users to conduct their analysis on prepared datasets, under strict security and data export controls.

The design principles are rooted in security-by-design, data protection by default, strict permit-based access, comprehensive auditability and integration within the broader CY-EHDS-2nd architecture detailed in *D5.1 Annex A: CY-EHDS-2nd Architecture and CP Infrastructure*. This includes reliance on the CPL for authentication and interaction with the DAAMs for permit information. Inspiration and practical insights have also been drawn from established SPE models in other EU Member States and through engagement with the European Health Data Space for the secondary use of health data (EHDS2) Community of Practice.

It should be noted that the requirements and specifications detailed in this document are expected to evolve in line with European developments. The content will be revised and updated once the deliverables from the TEHDAS2 and the official EHDS2 implementing acts become available, ensuring that the SPE implementation in Cyprus remains fully aligned with the latest EU guidance and legal requirements.

This document is structured as follows: Chapter 2 outlines the legal framework relevant to SPEs. Chapter 3 provides a landscape analysis of existing SPEs. Chapter 4 details the proposed CY-EHDS-2nd SPE Architecture, including roles, hosting model, and high-level design. Chapters 5 and 6 then delve into the specific requirements and technical specifications for the ISPE and ESPE respectively, followed by shared specifications. Chapter 7 explicitly details the alignment of this SPE framework with the EHDS Regulation. Finally, the document concludes with an outline of future plans and next steps for pilot implementation and operationalization.

The specifications herein will guide the development and pilot testing of the SPE, laying the groundwork for a secure, compliant, and effective health data infrastructure in Cyprus that supports critical secondary uses of health data while steadfastly upholding individual rights.

Figure 1 provides a high-level overview of the logical interactions between various human actors, the core components of the CY-EHDS-2nd infrastructure, and the specific information flows relevant to the (WP7). The diagram illustrates how the SPE (comprising the ISPE and ESPE) is integrated within the broader national architecture, emphasizing its dependencies on and interactions with other key modules such as the CPL and the DAAMs (WP5). The CY-EHDS-2nd SPE is highlighted as a centrally controlled and permit-driven environment, deeply integrated with the CPL for secure access and DAAMs for operational mandates, while ensuring auditable and secure data handling throughout its lifecycle. The set of interactions and flows depicted relevant to the SPE comprises:

1. **Actor Authentication via CPL:** All human actors interacting with SPE functionalities, including ISPE Operators and ESPE Operators (who configure and manage SPE instances) and Data Users (who access the ESPE for analysis), are authenticated through the CPL. The CPL utilizes its shared services (CPSS1: Identity and Access Management, CPSS2: User Profile & Accreditation, CPSS3: Role Management) to verify identities and roles before granting access to downstream SPE-related processes. All interactions are subject to CPSS4 (Logging, Monitoring & Audit). Note that ESPE Operators and Data Users require a Client Certificate for access.
2. **Permit Issuance by DAAMs (WP5):** The DAAMs module is responsible for managing health data access applications and issuing Data Permits. The diagram shows "Dataset Description" and "Data Permit" information flowing from DAAMs to the ISPE (WP7). This represents the critical permit parameters (e.g. authorised datasets, users, duration, purpose) that dictate the configuration and operation of specific SPE instances.
3. **ISPE (WP7) Operations:**
    - **Data Ingestion:** Data Holders upload datasets to the ISPE, a process facilitated by SPE Operators who require a Client Certificate for their actions.
    - **Data Preparation:** Within the ISPE, operators prepare datasets for the ESPE (e.g. pseudonymisation) or analyse data directly for data requests.
    - **Output to ESPE:** Prepared datasets, along with "Data Permit Metadata" and "Requested Dataset(s)" information, are made available from the ISPE to the corresponding ESPE instance.
4. **ESPE (WP7) Operations:**
    - **Configuration:** The ESPE is configured with the specific permit conditions by an ESPE Operator (requiring a Client Certificate).

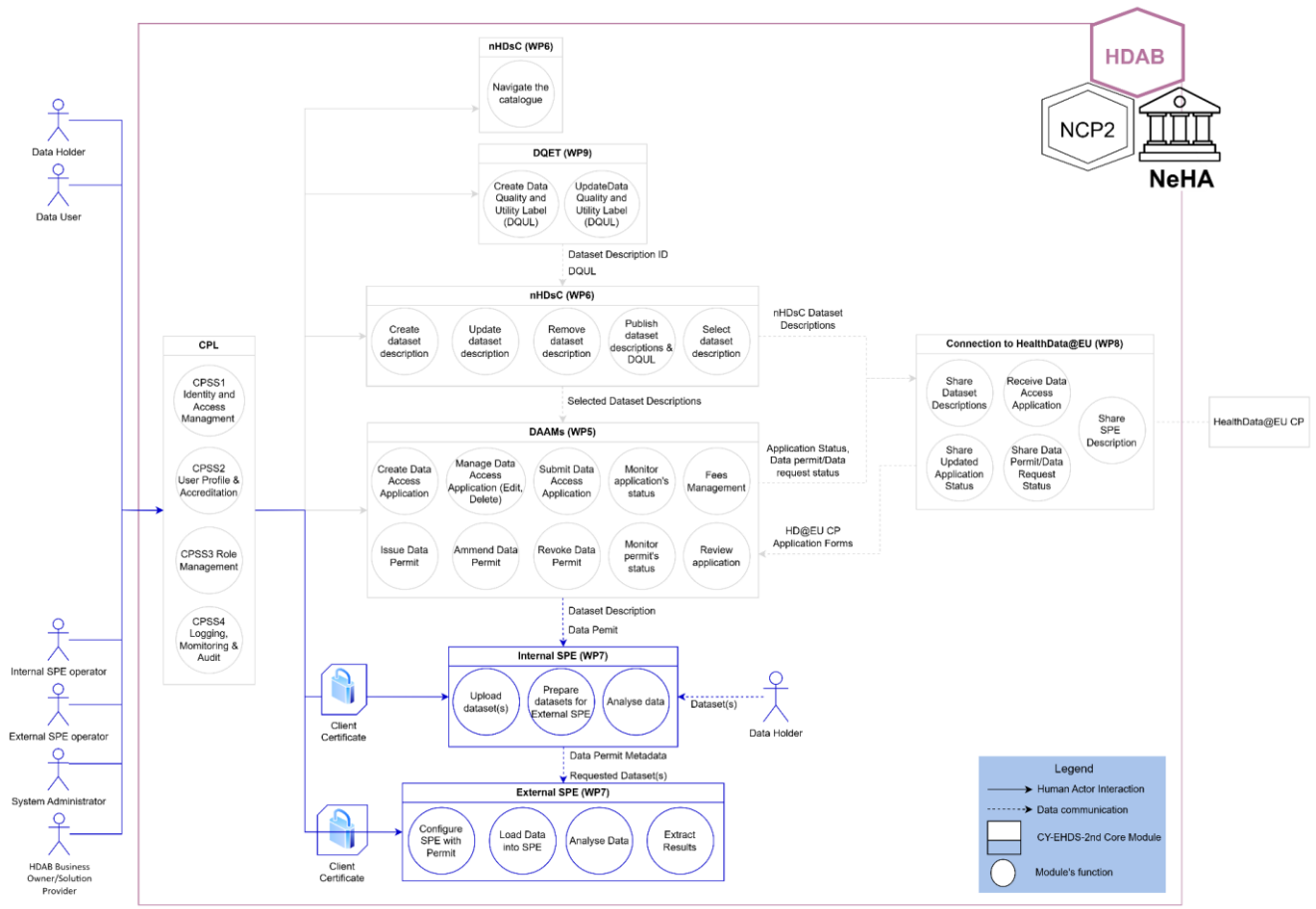

Figure 1: CY-EHDS-2nd SPE modules (as implemented in WP7)

- **Data Loading:** The prepared dataset from the ISPE is loaded into the permit-scoped ESPE instance.
- **Data Analysis:** Authorized Data Users (authenticated via CPL and Client Certificate) analyse data within their isolated ESPE.
- **Result Extraction:** Data Users can request to extract results, which are subject to review and control.

1.3 Objective of the Deliverable

The objective of this deliverable (D7.1 – SPE Requirements and Specifications) is to define the functional, non-functional, and technical requirements for implementing a national SPE in Cyprus, in alignment with the EHDS Regulation. This document provides the foundational specification for both the Internal and ESPE components, including architectural design, operational workflows, and compliance measures. As part of the broader CY-EHDS-2nd initiative, this deliverable directly supports the project's goal of enabling secure, privacy-preserving, and legally compliant secondary use of health data within the national infrastructure.

1.4 Connection with other Work Packages

The SPE, detailed in this deliverable, is a central component of the CY-EHDS-2nd infrastructure but does not operate in isolation. Its design, functionality and operation are intrinsically linked with, and often dependent upon, several other WPs that constitute the broader national architecture for the secondary use of health data, as outlined in *D5.1 Annex A: CY-EHDS-2nd Architecture and CP Infrastructure*. Understanding these interdependencies is crucial for a holistic view of the SPE's role:

- **CY-EHDS-2nd "D5.1 Annex A: CY-EHDS-2nd Architecture and CP Infrastructure":** This overarching document defines the entire national architecture, including the CPL and its shared services (CPSS1-CPSS4). The SPE (WP7) relies heavily on the CPL for:
  - User and Operator Authentication (CPSS1): All access to SPE instances is gated and authenticated by the CPL, utilizing CY Login and mutual Transport Layer Security (mTLS) client certificates.
  - Role Management and Authorization (CPSS3): The CPL validates high-level roles before routing users/operators to SPE resources.
  - Centralized Audit Logging (CPSS4): SPE-generated audit logs are integrated with the central observability stack managed under CPL governance. D7.1 therefore specifies how the SPE interfaces with and consumes these critical CPL services.
- **WP5 (DAAMs):** The DAAMs is responsible for managing health data access applications and issuing data permits or approving data requests. The SPE operation is directly driven by the outputs of DAAMs:
  - Approved data permits dictate the scope, authorized users, datasets, duration and tools for each ESPE instance.
  - Approved data requests inform the processing tasks undertaken within the ISPE to generate statistical outputs. This deliverable (D7.1) describes how SPE instances are configured based on permit information originating from DAAMs, currently facilitated by the HDAB Data Permit

Manager, with a view towards future Application Programming Interface (API)-based integration.

- More information about the requirements and specifications of CY-EHDS-2nd DAAMs can be found in the project's deliverable "D5.1 DAAMs Requirements, Specifications and Prototype".

- **WP6 nHDsC:** The nHDsC provides the metadata for datasets available for secondary use. While the SPE does not directly interface with the nHDsC for its operational tasks (as dataset selection occurs during the DAAMs application process), the datasets provisioned within the SPE will correspond to those catalogued in the nHDsC. The deliverable CY-EHDS-2nd "D6.1 nHDsC Requirements and Specifications" provides more insight into the nHDsC requirements and specifications.

2 LEGAL FRAMEWORK

The European legal framework underpinning the SPEs and their implementation within the Cypriot context for the secondary use of electronic health data, as facilitated by the CY-EHDS-2nd project.

2.1 European Legal Framework for Secure Processing Environments

SPEs are a cornerstone of the EHDS Regulation [8], providing the mandatory legal and technical infrastructure for privacy-preserving access to electronic health data for secondary use.

- **Primary Legal Basis: The EHDS Regulation**

  It establishes the SPE as the sole lawful environment for natural persons to process non-anonymised electronic health data for secondary use. This is principally codified in Article 73 SPE of the Regulation, which mandates specific technical, security, and procedural guarantees that SPE operators must implement. The main obligations derived from Article 73 include:

  - Restricted and Authorised Access: Access to the SPE must be strictly limited to authorised natural persons listed in the data permit (Article 73(1)(a)). Health data users must only have access to electronic health data covered by their data permit, enforced through individual and unique user identities and confidential access modes (Article 73(1)(d)).
  - Data Protection and Security Measures:
    - SPEs must implement state-of-the-art technical and organisational measures to minimise the risk of unauthorised reading, copying, modification, or removal of electronic health data hosted within (Article 73(1)(b)).
    - The input, inspection, modification, or deletion of electronic health data within the SPE must be limited to a restricted number of authorised, identifiable individuals (Article 73(1)(c)).
  - Logging and Auditing: Identifiable logs of all access to and activities within the SPE must be kept for a period necessary for verification and auditing, with access logs retained for at least one year (Article 73(1)(e)).
  - Compliance Monitoring and Threat Mitigation: SPEs must ensure ongoing compliance with and monitoring of these security measures to mitigate potential security threats (Article 73(1)(f)).
  - Data Upload and Download Control: HDABs must ensure electronic health data can be uploaded by data holders and accessed by users within the SPE. Crucially, they must review

download requests to ensure only non-personal electronic health data (including anonymised statistical format) is downloaded from the SPE (Article 73(2)).
- Regular Audits: HDABs are required to ensure regular audits of the SPEs, including by third parties, and to take corrective actions for any identified shortcomings (Article 73(3)).
- Commission Implementing Acts: The EC is mandated to adopt implementing acts by [Date from Article 73(5) - e.g., 26 March 2027] specifying common technical, organisational, information security, confidentiality, data protection, and interoperability requirements for SPEs (Article 73(5)).

These provisions of Article 73 establish SPEs not merely as technical solutions but as integral compliance mechanisms, ensuring the lawful and secure processing of sensitive health data under a robust governance framework.

- **Overarching Compliance: GDPR**
  While the EHDS Regulation provides the sector-specific legal framework, the (EU) 2016/679 GDPR continues to apply horizontally. SPEs, as defined by Article 73 of the EHDS Regulation, directly support compliance with core GDPR principles, notably:
  - Data minimisation
  - Integrity and confidentiality
  - Security of processing
  - The responsibility of the controller to implement appropriate technical and organisational measures, which the SPE helps to fulfill.

  The SPE infrastructure enables HDABs (acting as data controllers for the purpose of granting access) to fulfill their GDPR obligations effectively.
- **Interplay with Other EU Data Governance Instruments:**
  The EHDS Regulation and its provisions for SPEs operate within the broader EU data strategy, complementing other key legislative acts such as the Data Governance Act (DGA) (Regulation (EU) 2022/868, which is also referenced in Article 73(4) concerning data altruism organisations) and the upcoming Data Act.

2.2 National Implementation Context under CY-EHDS-2nd (Cyprus)

- **Current National Legal Standing:**

  Currently, Cyprus is in the process of transposing and fully aligning its national legal framework with the requirements of the EHDS Regulation. While specific national legislation detailing SPE operations is under development, the EHDS Regulation itself, once fully applicable, along with the GDPR, will provide the direct legal basis for the establishment and operation of the SPE infrastructure within Cyprus.

- **Role of NeHA and CY-EHDS-2nd:**

  Under this European legal framework, the NeHA is designated as the HDAB for Cyprus. As such, NeHA will be responsible for operating the national SPE infrastructure. The CY-EHDS-2nd project, including its WP8 National Connector, is tasked with developing the technical capabilities to operationalize these SPE functionalities in strict adherence to EU legal requirements. All governance, access control, security measures, and operational procedures for the Cypriot SPE will be derived from and comply with the EHDS Regulation (particularly Article 73) and the GDPR.

- **Commitment to Future Legal and Regulatory Alignment:**

Cyprus is committed to ensuring continuous alignment with the evolving EU legal landscape for health data. This includes:

- Proactive preparation for and adoption of the upcoming Implementing Acts by the EC concerning common SPE requirements (as per Article 73(5) of the EHDS Regulation).
- Full incorporation of amendments to the national eHealth law once enacted, which will further detail the legal provisions for SPE establishment, certification, and operation in Cyprus.
- Adherence to implementation guidelines and technical specifications emerging from EU-level initiatives such as TEHDAS2 and the ongoing guidance from the HealthData@EU CP infrastructure.

3 LANDSCAPE ANALYSIS

3.1 SPEs in Cyprus

In Cyprus there are no SPEs so far, neither provided by NeHA as the national single HDAB of Cyprus nor by other organisations/bodies. In the context of the CY-EHDS-2nd project we will implement the availability of NeHA providing SPE to CY-EHDS-2nd data users as part of the national secondary use of health data in Cyprus.

3.2 SPEs in the European Union

A limited number of EU Member States currently operate fully functional and legally supported SPEs for the secondary use of electronic health data. This section presents three mature and active SPE implementations that serve as key reference points for the design of the SPE component in the CY-EHDS-2nd architecture. Each example is selected based on its legal mandate, operational maturity, and publicly documented compliance with data protection and security requirements.

3.2.1 Finland – Kapseli (Findata)

Findata is Finland's national Social and Health Data Permit Authority, established in 2019 under the Act on the Secondary Use of Health and Social Data (552/2019). It serves as the centralized body responsible for granting permits for secondary use of health and social data, collecting and combining data from various sources, and providing access through secure environments. To facilitate secure data processing, Findata offers Kapseli, a SPE that allows authorised users to access and analyse data without compromising privacy.

To further enhance its infrastructure, Findata launched the FinHITS project (Strengthening Finnish Health Data ICT for Secondary Use)[5], a four-year initiative co-funded by the EU under the EU4Health program. The project aims to improve data access services, develop the national dataset catalogue, strengthen the SPE, and establish a cross-border gateway (XBG) to connect with the HealthData@EU infrastructure [11].

- **Operator**: Findata – Finnish Social and Health Data Permit Authority
- **Operational Since**: April 2020
- **Legal Basis**: Act on the Secondary Use of Health and Social Data (552/2019)

[5] https://findata.fi/en/finhits/#:~:text=Through%20FinHITS%2C%20we%20are%20strengthening,integrate%20seamlessly%20into%20the%20EHDS.

- **Hosting Model**: On-premise infrastructure
- **Access Method**: Remote desktop session via web browser with 2FA
- **Internet Access**: Not permitted; the SPE operates under full network isolation
- **Target Users**: Authorised individuals under an approved data permit
- **Data Export**: Exports require manual approval by Findata
- **Confirmed Usage:**
  - 147 active Kapseli environments and 875 registered users as of end-2024
  - 113 Kapseli environments and 830 users recorded in 2022

3.2.2 France – Health Data Hub Public Interest Grouping

The Health Data Hub (HDH) is a public interest group established by the French government to facilitate access to health data for research and innovation. It provides a centralized platform that aggregates various health data sources and offers secure access through a cloud-based infrastructure. The HDH operates under the oversight of the French data protection authority (CNIL) and complies with national regulations governing health data usage [12].

- **Operator**: Public Interest Grouping (GIP) HDH
- **Operational Since**: December 2019
- **Legal Basis**: Established by Ministerial Decree; subject to CNIL oversight
- **Hosting Model**: Hosted in Microsoft Azure France (HDS-certified health data cloud)
- **Access Method**: Secure virtual containers with identity verification
- **Internet Access**: Not available from within the analysis environment
- **Target Users**: Approved researchers and institutions
- **Data Export**: Exports require formal review and approval

3.2.3 Belgium – Healthdata.be (Sciensano)

Healthdata.be is managed by Sciensano, Belgium's national institute for health. It serves as a centralized platform for collecting, managing, and providing access to health data for research and policymaking. The platform ensures data security and privacy through controlled access and compliance with national regulations [13].

- Operator: Sciensano – Belgium's public health institute
- Operational Since: 2017
- Legal Basis: Royal Decree governing reuse of health data
- Hosting Model: On-premise secure infrastructure
- Access Method: Institutional user access through Sciensano’s portal with authentication controls
- Internet Access: Not permitted during processing
- Target Users: Registered researchers from certified institutions

- Data Export: Exports are subject to formal review by Sciensano

3.2.4 *Future SPE under HealthData@EU*

The EC is establishing a common SPE under the HealthData@EU infrastructure, which will enable secure, cross-border access to datasets under multicounty data permits [3-7]. This EU-level SPE will be operated and certified in accordance with implementing acts under Article 73(5) of the EHDS Regulation.

As of this writing, the HealthData@EU SPE is not yet operational, and the related technical specifications from TEHDAS2 and the Commission have not been formally adopted.

3.2.5 *CY-EHDS-2nd Design Alignment*

As the implementing acts under Article 73(5) of the EHDS Regulation are still under development, CY-EHDS-2nd will align its national SPE requirements and specifications as soon as these acts are formally adopted. In the interim, the project is closely observing the outcomes of WP7 of the TEHDAS2 Joint Action, which specifically addresses the functional and technical characteristics of SPEs under the EHDS framework.

In parallel, CY-EHDS-2nd intends to leverage technical documentation, governance frameworks, and reference architectures published through the HealthData@EU infrastructure [3-7], including any future guidance related to the EU-level SPE for multi-country data permits.

Until these resources are finalised, the project is actively monitoring the implementation experiences of Member States that already operate SPEs successfully, such as Finland, France, and Belgium. Their input, operational feedback, and shared best practices, particularly as disseminated through the EHDS2 Community of Practice, serve as valuable references to inform the initial national design and technical specifications.

4 CY-EHDS-2ND SPE ARCHITECTURE

CY-EHDS-2nd SPE architecture is designed to ensure the secure, isolated, and auditable processing of electronic health data for secondary use in accordance with Article 73 of the EHDS Regulation and the overall CY-EHDS-2nd system architecture. The SPE component consists of two logically separated environments operated by NeHA:

- **ISPE**: used exclusively by authorised operators of NeHA to process raw datasets received from data holders. Its outputs are either statistical (for data requests) or pseudonymised datasets (for data permits).
- **ESPE**: provisioned by NeHA for approved data users named in a data permit, who analyse pre-processed datasets in a secure, isolated workspace.

Each environment is deployed on infrastructure which is managed by NeHA and follows strict access control, traceability, and security requirements. SPEs do not have access to the internet and are isolated from other infrastructure components except through controlled orchestration layers.

The CY-EHDS-2nd SPEs operate as an integral component within the overall CY-EHDS-2nd infrastructure, the architecture of which is detailed in CY-EHDS-2nd *D5.1 Annex A: CY-EHDS-2nd Architecture and CP Infrastructure*. The SPE relies on the CY-EHDS-2nd CPL for foundational services, notably for the authentication of all personnel accessing SPE instances (both ISPE Operators and ESPE Data Users) via CY Login, and for initial high-level role validation. The CPL acts as the secure gateway before users or operators

are directed to the appropriate SPE resources, ensuring a consistent identity and access management approach across the entire CY-EHDS-2nd ecosystem.

4.1 Roles and Actors

The complete set of actors and their responsibilities across the CY-EHDS-2nd infrastructure is defined in *D5.1 – Annex D: Common Actor Definitions – CY-EHDS-2nd (v1.0)*. That annex serves as the single authoritative reference for roles appearing in Work Packages 5 to 9, ensuring alignment with the EHDS Regulation and the implementation scope agreed by NeHA.

Table 2 below presents only the actors relevant to this module. These have been selected from the common list based on their participation in the workflows and responsibilities specific to this work package.

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

Actor No.	Role
A2	Data User
A3	Data Holder
A10	Internal SPE Operator (ISPE Operator)
A11	External SPE Operator (ESPE Operator)
A31	HDAB Business Owner / Solution Provider

4.2 SPE National Hosting Model

In the framework of CY-EHDS-2nd, the SPE infrastructure is hosted and operated entirely by NeHA, the national HDAB. NeHA is responsible for provisioning, maintaining, and securing two distinct environments presented in Table 3, each aligned to a specific phase of the secondary data lifecycle:

- The ISPE, used for data preparation and transformation by authorised NeHA personnel
- The ESPE, accessed by data users explicitly named in an approved data permit

The SPE architecture ensures that:

- All electronic health data are processed and stored exclusively within the jurisdiction of the Republic of Cyprus
- Processing activities are fully auditable, access-controlled, and traceable end-to-end
- There is a clear functional separation between internal dataset preparation and external data analysis

As the sole SPE operator in Cyprus, NeHA governs both environments under a unified set of:

- Security and access control policies
- Logging and monitoring frameworks
- Incident detection and response procedures

Table 2: CY-EHDS-2nd SPE types

SPE Type	Hosting Responsibility	Purpose	Location
ISPE	NeHA	Used exclusively by internal NeHA personnel (SPE Operators) to process raw data provided by data holders and generate datasets or statistical outputs.	National infrastructure managed by NeHA (final infrastructure hosting model to be updated)
ESPE	NeHA	Provides a secure analysis environment for authorised data users named in an approved data permit.	National infrastructure managed by NeHA (final infrastructure hosting model to be updated)

Each SPE instance is:

- Network--isolated from all other services
- Provisioned as a dedicated environment per data permit or data request
- Managed through automated lifecycle controls, including secure start, monitoring, and teardown

In accordance with Article 68(12) of EHDS regulation, Internal and ESPE environments are ephemeral. They are destroyed no later than six months after the expiry of the corresponding data permit. Processing formulas may be retained by NeHA upon request of the data user.

4.3 High Level SPE Architecture

The SPE in CY-EHDS-2nd is architected as a two-tier, environment-based system operated exclusively by NeHA, with strict permit-scoped access and full alignment to the legal, technical, and security provisions of the EHDS Regulation.

At the core of the architecture are two isolated environments:

- The ISPE, used by NeHA operators to ingest raw data from data holders and prepare outputs.
- The ESPE, made available to authorised data users for analysis, based on the scope defined in an approved data permit.

In this context, the CY-EHDS-2nd architecture adheres to the following core principles:

- **Permit-scoped isolation**
  Each SPE instance (Internal or External) is instantiated as a dedicated virtual machine (VM) per data permit or data request.
- **Lifecycle enforcement**
  VMs are automatically destroyed no later than six months after the expiry of the corresponding permit, in accordance with EHDS Article 68(12).
- **Network segmentation**
  Both SPEs are isolated from the public internet, with tightly controlled ingress and egress channels.
- **CPL integration**
  All access to ESPEs is mediated via the CPL (CPSS1/CPSS3), ensuring mature authentication, role resolution, and session scoping.

- **Logging and observability**
  Both Internal and ESPEs push structured logs to the central CPSS4 logging stack. Manual actions by operators are logged via NeHA-controlled systems.
- **Secure data flow**
  ISPEs receive datasets from data holders via SFTP. Processed results are either uploaded to the ESPE or exported via email for statistical requests.

4.3.1 Components

The components listed below represent the elements that are directly provisioned, operated, or governed under WP7 SPE. Cross-cutting services such as authentication, access control, session routing, and logging are handled by the CY-EHDS-2nd CPL and are described separately in the CY-EHDS-2nd General Infrastructure deliverable[6]. Table 3 provides a structured overview of the SPE related components and their respective responsibilities.

Table 3: CY-EHDS-2nd SPE Architecture Components

Component	Type	Description	Responsible Entity
ISPE VM	Internal	Dedicated, isolated VM used by NeHA operators to process raw data from data holders	NeHA (ISPE Operator)
ESPE VM	External	Dedicated, browser-accessible VM made available to authorised data users	NeHA (ESPE Operator)
SFTP Ingestion Service	Shared (Ingress)	Secure transfer service used by data holders to deliver datasets to the ISPE	NeHA (Ops / Infra)
Permit Metadata Input	Shared (Control)	Manual input channel used by the Data Permit Manager to configure SPEs based on approved permits	NeHA (Data Permit Manager)
Export Control Layer	Internal	Manual result validation and export mechanism for data requests and processed datasets	NeHA (SPE Operator)
Script Vault	Internal	Optional retention component storing user-requested processing logic from the ISPE	NeHA (Governance Unit)

Each component listed in Table 3 plays a distinct role in the secure, data permit-scoped operation of the SPE infrastructure. The subsections below provide a clear and formal description of their responsibilities and interactions within the broader CY-EHDS-2nd architecture.

4.3.1.1 ISPE VM

The ISPE is instantiated as a VM that is provisioned per data permit or request. It is accessed exclusively by authorised NeHA personnel acting as ISPE Operators. Its primary function is to receive raw datasets from data holders and process them to generate either pseudonymised datasets (in the case of data permits) or statistical results (in the case of data requests). The environment is air-gapped, network-isolated, and equipped with approved analytical tools. It operates under NeHA direct control and enforces full traceability of all actions.

[6] WP7 relies on the CPL shared services (CPSS1–4) for secure authentication, role-based authorisation, session enforcement, and audit logging. These orchestration and identity services are not re-implemented under WP7 but are integrated with SPE workflows.

4.3.1.2 ESPE VM

The ESPE is a VM provisioned for each approved data permit and made accessible to the data users explicitly named in that permit. It offers a browser-based, session-isolated remote desktop environment, accessible only through strong authentication mechanisms (CY Login and client certificate). Data users are authorised to analyse datasets prepared by NeHA but are technically prevented from copying, downloading, or exporting any data unless explicitly permitted. The ESPE is also network-isolated and configured per permit-specific constraints.

4.3.1.3 SFTP Ingestion Service

The SFTP service enables data holders to securely transmit the datasets referenced in the permit to NeHA. Each data holder is assigned a logically isolated workspace within a centralised SFTP system, scoped per permit and enforced through access control lists (ACLs). This design allows for efficient and secure data ingestion while ensuring full segregation, logging, and auditability of all dataset transfers.

4.3.1.4 Permit Metadata Input (via Data Permit Manager)

During the initial implementation phase, permit configuration and lifecycle monitoring are handled manually by a designated NeHA officer, referred to as the Data Permit Manager. Upon permit approval, this officer extracts the relevant operational parameters (authorised users, permitted datasets, duration, access rights) and communicates them to SPE Operators via secure internal channels. This manual coordination mechanism ensures that each SPE instance is correctly provisioned in accordance with the legal and technical constraints of the permit.

4.3.1.5 Export Control Layer

The export of results from the SPE infrastructure is governed by a strict manual validation process. For data requests, statistical outputs generated in the ISPE are reviewed by NeHA personnel before being released to the requesting data user. For data permits, NeHA transfers the processed dataset to the ESPE, where the data user can analyse it in situ. At no point can data be copied or extracted from the ESPE unless authorised in the permit and approved by NeHA. This control mechanism ensures full compliance with Article 73(1)(b) of the EHDS Regulation.

4.3.1.6 Script Vault

The Script is an internal service that enables the storage of user-requested processing scripts or computational formulas used within the ISPE. This feature supports Article 68(12) of the EHDS Regulation, which permits the retention of such formulas at the user's request. The vault will support version control, tagging, and association with specific permits and datasets, ensuring reproducibility while maintaining data minimisation and confidentiality principles.

4.4 Compliance and Future Alignment

Both the Internal and ESPEs are deployed under a strict security model fully aligned with Article 73 of the EHDS Regulation. This includes full network isolation (no internet access), strong user authentication (via CPL), and internal enforcement of zero trust principles, including least-privilege access, logical segmentation, and continuous verification. These measures ensure that all data processing within the SPE remains secure, auditable, and privacy-preserving.

The current architecture is explicitly designed to comply with the future implementing acts of the EC (Article 73(5)), which will define common security, interoperability, and certification criteria for SPEs across Member

States. It also supports horizontal scalability and future onboarding of additional authorised SPE operators, if so permitted under the amended national law.

4.5 Operational Lifecycle and Information Flow

The lifecycle of each SPE instance under CY-EHDS-2nd is directly tied to a formally approved data permit or data request, issued by DAAMs (WP5). Each data permit or request is assigned to a unique reference ID, which serves as the traceability anchor across all subsequent operations: data ingestion, processing, access, output delivery, and lifecycle management. All SPE operations are initiated, governed, and terminated under the responsibility of HDAB (NeHA).

4.5.1 Step 1 – Permit Approval and Configuration

The SPE lifecycle is initiated upon the formal approval of a data permit or data request within the CY-EHDS-2nd DAAMs detailed in the deliverable D5.1 DAAMs Requirements, Specifications and Prototype and *D5.1 Annex A: CY-EHDS-2nd Architecture and CP Infrastructure*. DAAMs serves as the authoritative source for all permit conditions and assigns a unique reference ID to each approved application, ensuring traceability.

Following approval in DAAMs, the HDAB Data Permit Manager is responsible for extracting the critical operational parameters from the approved permit. These parameters are essential for the correct and compliant configuration of the SPE instances. Table **4** presents the key parameters recorded so far for this process while any other specific security, processing, or handling constraints mandated by the permit will be added during the implementation phase.

Table 4: Data Permit and Other Key Parameters required for the initiation of the SPE lifecycle

Data Permit Key Parameter	Details
Unique Permit/Request ID	Received from DAAMs
Authorised Data Users	For ESPEs, a definitive list of named individuals permitted access.
Authorised SPE Operators	For ISPE tasks related to this permit.
Referenced Datasets	Specific dataset identifiers (e.g., from the nHDsC, WP6) and the corresponding Data Holders.
Permit Validity Period	Start and end dates for SPE access/data processing.
Approved Analytical Tools	A specific list of software and tools permitted for use within the SPE (especially for ESPEs).
Data Processing Instructions/Scope	For ISPE, any specific transformation, pseudonymisation, or aggregation requirements. For ESPE, the defined scope of analysis.
Output Type and Delivery	Whether the output is a prepared dataset for an ESPE or statistical results for direct delivery.
Export Rules and Restrictions	Conditions under which results may be exported from an ESPE.

For the initial operational phase of CY-EHDS-2nd, the HDAB Data Permit Manager securely communicates these parameters to the designated Internal and/or ESPE Operators (e.g. via encrypted email using a standardized template). The SPE Operators then manually configure the respective SPE instance according to these precise instructions. Regarding data processing instructions for ISPE, any specific transformation, pseudonymisation, or aggregation requirements must be prescribed while for ESPE, the defined scope of analysis. For the output type and the output delivery instructions must include whether the output is a prepared dataset for an ESPE or statistical results for direct delivery while the conditions under which results may be exported from an ESPE must be also included. Overall, all the specific security, processing, or handling constraints mandated by the permit must be clearly defined during implementation.

This configuration, driven by the approved permit provide dby DAAMs, ensures that all subsequent SPE operations adhere strictly to the authorised scope and conditions. Future enhancements aim to automate this DAAMs-SPE information interface via secure APIs for greater efficiency and reduced manual intervention.

4.5.2 Step 2 – Dataset Upload by Data Holders via Secure SFTP

Upon instruction (originating from the approved data permit and communicated via HDAB Data Permit Manager), designated Data Holders are required to upload the specified electronic health datasets to the CY-EHDS-2nd infrastructure. This upload is facilitated through a secure SFTP service managed by NeHA as part of the ISPE's data ingestion capabilities. Key aspects of this step include:

- Permit-Scoped Workspaces: Each Data Holder is provided with access credentials to a unique, logically isolated SFTP workspace (e.g., a dedicated directory) specifically assigned to their organization and the relevant data permit ID. Access is time-bound and strictly controlled.
- Data Integrity and Traceability: Upload mechanisms should support verification of data integrity (e.g. via checksums if specified by NeHA). All SFTP upload activities (logins, files transferred, timestamps) are logged to the central observability stack, ensuring a full audit trace of data ingress and its binding to the specific data permit.
- NeHA Supervision: While Data Holders perform the upload, the process is managed and supervised by NeHA to ensure compliance with security and procedural requirements.

No dataset can be uploaded outside this controlled and audited flow, ensuring separation between data holders and clear linkage of data to its originating permit.

4.5.3 Step 3 – ISPE Processing

Ingest the raw dataset(s), perform cleaning, apply pseudonymization techniques as required, transform data into the specified analytical format, and prepare the final dataset according to the conditions and scope defined in the data permit (communicated by the HDAB Data Permit Manager).

Authorised NeHA operators access the ISPE using CY Login and client certificates. Within the ISPE:

- For data permits: Ingest the raw dataset(s), perform cleaning, apply pseudonymization techniques as required, transform data into the specified analytical format, and prepare the final dataset according to the conditions and scope defined in the data permit (communicated by the HDAB Data Permit Manager).
- For data requests: Execute predefined statistical procedures or queries on the relevant datasets to generate the requested aggregated, non-identifiable statistical outputs.

All processing actions are conducted using only whitelisted tools approved by HDAB (NeHA) within this highly secure and network-isolated environment. Every significant operator action and data transformation step is logged centrally in compliance with EHDS Article 73(1)(e) and integrated with the CY-EHDS-2nd shared observability stack.

4.5.4 Step 4 – Secure Output Delivery by ISPE Operators

Following data processing within the ISPE (Step 3), the method of output handling by the authorised NeHA ISPE Operator is determined by the nature of the approved application (data permit or data request):

- **For Data Permits (leading to ESPE access):**

- The ISPE Operator conducts a final review and validation of the prepared (e.g. pseudonymised) dataset to ensure it aligns with the permit conditions and contains no directly identifying information not explicitly authorised for transfer.
- The validated dataset is then securely transferred via a NeHA-controlled internal mechanism from the ISPE to the specifically provisioned, isolated ESPE VM. This VM is designated for the authorised Data Users listed in that particular data permit. This transfer is logged.

- **For Data Requests (statistical output):**
  - The ISPE Operator validates that the generated statistical results are aggregated, anonymized, and fully comply with the data request's scope and the conditions of the approved application, ensuring no re-identification risk.
  - The validated, non-personal statistical output is then transmitted to the original requester via a secure delivery mechanism defined by NeHA (e.g. encrypted email). This delivery is logged.

In both scenarios, no raw or unauthorised data is released outside of NeHA-controlled environments or processes.

4.5.5 Step 5 – ESPE Access (Data Permits Only)

For data permits, the ESPE is provisioned as a remote VM for each permitted data user. Key properties include:

- Access only via CY Login + 2FA and client certificate
- Sandbox environment with no internet access
- Pre-installed analytical tools (e.g. RStudio, Python, LibreOffice offline)
- Read-only access to the prepared dataset
- No ability to export raw data from the environment

If result extraction is permitted, it is logged and reviewed before release.

4.5.6 Step 6 – Audit Logging and Traceability

Audit logging within the SPEs is a critical function for ensuring traceability, compliance, and security. SPE instances generate logs for key operational and user activities. These SPE-generated logs are designed for integration with the central CY-EHDS-2nd observability stack, which is managed by the CPL(CPSS4) as detailed in CY-EHDS-2nd *D5.1 Annex A: CY-EHDS-2nd Architecture and CP Infrastructure.* This ensures that SPE activities form part of the comprehensive, platform-wide audit trail.

While the commitment to this central integration is firm, the specific technical protocols for log transmission, the detailed list of SPE-specific auditable events, and the precise log formats will be finalised during the detailed design and pilot implementation phase. This will ensure alignment with emerging TEHDAS2 technical specifications for SPEs and the eventual EHDS Implementing Acts regarding audit and monitoring requirements. In general, all actions across the SPE lifecycle MUST be logged centrally. This includes but not limited to:

- Dataset uploads

- Operator access and transformations
- ESPE logins
- File movements and result deliveries

Logs are linked to the unique permit or request ID and include timestamps, user identifiers and system actions.

4.5.7 Step 7 – SPE Decommissioning, Data Deletion, and Retention

Upon the expiration or termination of a data permit, the lifecycle of the associated SPE resources is managed to ensure compliance with EHDS Regulation Article 68(12) and data minimisation principles:

- SPE VM Decommissioning: All SPE VMs (both ISPE resources used for that permit and any associated ESPE VM) are marked for destruction. The electronic health data processed within these environments for that permit must be securely deleted no later than six months after the expiry of the data permit.
- Secure Deletion: This includes the secure wiping of all datasets, intermediate processing files, and temporary user data from the SPE VMs and associated storage. The deletion process itself is logged.
- Script/Formula Retention (Script Vault): As per EHDS Article 68(12), upon request of the Health Data User (for data permits) and subject to NeHA governance and approval, computational scripts or processing logic (formulas) used to create the requested dataset within the ISPE may be retained by NeHA in the secure 'Script Vault'. This retained logic must not contain personal data and serves as a reproducible record for potential future verification or re-use under a new, valid data permit. Access to the Script Vault is strictly controlled by NeHA.
- Audit Log Retention: Audit logs pertaining to the SPE instance and its activities are retained according to defined policies (see Step 6), independently of the SPE VM data deletion.

5 INTERNAL SECURE PROCESSING ENVIRONMENT

The ISPE is a virtualised, isolated computing environment operated solely by NeHA for the preparation and transformation of datasets received from data holders under an approved data permit or data request. It constitutes the first tier of the national SPE architecture under CY-EHDS-2nd and is a mandatory component in both access modalities defined in the EHDS Regulation (i.e. data permits and data requests).

The ISPE is not directly accessible to external data users. Instead, it is accessed exclusively by authorised NeHA personnel (ISPE Operators), who are responsible for performing all operations defined in the permit or request, including:

- Data ingestion and verification
- Cleaning, transformation, and pseudonymisation
- Statistical analysis (in the case of data requests)
- Preparation of datasets for transfer to the ESPE (in the case of data permits)

All ISPE s are instantiated as VMs with particular data permit or data request scope. Each VM is bound to a unique data permit or request ID and is provisioned only for the duration of that access right, plus a six-

month retention period as mandated by Article 68(12) of the EHDS Regulation. At the end of this period, the VM is automatically decommissioned and destroyed.

The ISPE is deployed on national infrastructure managed by NeHA. It operates in a network-isolated environment with no inbound or outbound internet connectivity, enforcing the strict security controls and data minimisation principles required under EHDS Article 73 and GDPR. All interactions within the ISPE are authenticated via CY Login and client certificate (mutual TLS), and every operation is logged and linked to the corresponding permit ID through the central audit infrastructure.

The ISPE supports only controlled, in-scope processing. No data export or user access is allowed beyond the boundaries established by the approved data permit/data request. If needed, NeHA may retain processing formulas or computational logic within the Script Vault component.

5.1 Actors and Interfaces

The ISPE operates as a secure, virtualised environment built per data permit/data request, accessed and managed exclusively by authorised NeHA personnel. It is not accessible by data users or third parties. Its interactions involve a limited number of actors, all of whom are bound by distinct responsibilities and interface access methods. These roles are governed by the approved data permit or data request and enforced via authentication and traceability mechanisms as required under Article 73 of the EHDS Regulation.

The tables below Table **5**, Table **6** provide a structured overview of (a) the key actors involved in the ISPE lifecycle (as defined in *D5.1 Annex D: Common Actor Definitions – CY-EHDS-2nd (v1.0)*) and (b) the specific technical interfaces and authentication mechanisms through which each actor interacts with the SPE infrastructure. This separation ensures full transparency over role boundaries, technical control points, and governance dependencies.

Table 5: ISPE Actors and their Responsibilities as defined in *D5.1 Annex D: Common Actor Definitions – CY-EHDS-2nd (v1.0)*

Actor No.	Actor
A3	Data Holder
A5	Data Permit Manager
A10	Internal SPE Operator
A31	HDAB Business Owner / Solution Provider

It is important to note that no external data user has access to the ISPE. Their access is limited to the ESPE, which is provisioned separately per data permit.

Table 6: Actor Interfaces and Access Mechanisms

Actor	System Interface Used	Interface Description
Data Permit Manager	Encrypted email with standard configuration template	Used to transmit the operational configuration of each approved data permit or request to SPE Operators. The message includes a fixed-format template describing permitted datasets, access duration, authorised users, and output handling rules. This process is manually overseen. The communication method may evolve into a formal permit registry API in future phases.

ISPE Operator	Remote desktop to permit-scoped VM via CY Login + client certificate	Operators log in to each ISPE VM using strong authentication and pre-assigned credentials. All access is logged centrally.
Data Holder	SFTP endpoint, scoped per permit	Permit-scoped drop zone with ACLs and time-bound access. Files are isolated and logged per holder and permit.

All interface channels are secured using encrypted transport and where applicable mature authentication. Interfaces are restricted by role, time window, and permit ID to ensure strict adherence to access boundaries.

5.2 Workflow

The ISPE workflow is activated upon the approval of a data permit or data request and follows a structured, traceable sequence of operations under the supervision of NeHA. The entire process is bounded by the conditions defined in the approved access request and enforced through manual and system-level controls.

Table **7** outlines the internal workflow executed by NeHA personnel within the ISPE, highlighting each step, the responsible actor, and the input/output artefacts at each stage. Although workflow orchestration is currently managed manually, the execution path is designed to support lifecycle traceability, data minimisation, and strict compliance with Article 68 and Article 73 of the EHDS Regulation. The workflow applies to both data permits and data requests, with branching logic at Steps 6a and 6b depending on the type of request. All actions within this workflow are fully logged in the central audit system, and the traceability of every input and output is linked to the unique permit or request ID issued via DAAMs.

Table 7: ISPE Workflow Overview

Step	Action	Actor	Input	Output
1	Receive data permit or data request configuration	Data Permit Manager	Approved data permit or data request (from DAAMs)	Encrypted email with configuration template sent to ISPE Operator
2	Prepare SPE environment	ISPE Operator	Configuration template, internal SOPs	Provisioned VM, ready for dataset ingestion
3	Ingest datasets via SFTP	ISPE Operator	Uploaded files from SFTP workspace	Verified and locally stored dataset in ISPE
4	Process dataset	ISPE Operator	Raw dataset, processing tools	Pseudonymised dataset (for permit) or statistical output (for request)
5	Review and validate results	ISPE Operator	Output files	Approved dataset or statistical result
6a	Transfer dataset to ESPE (permit)	ISPE Operator	Finalised dataset	Dataset loaded to ESPE VM (read-only)

6b	Send statistical result to requester (request)	ISPE Operator	Aggregate output	Email sent to data user
7	Store scripts (if applicable)	ISPE Operator	User-requested processing formulas	Saved to Script Vault (optional)
8	Decommission VM	Lifecycle Controller + NeHA	Permit expiry + 6 months	SPE VM destroyed, logs retained

5.3 Functional Requirements

The following FRs govern the ISPE component of CY-EHDS-2nd. Each requirement is tied to one or more authorised workflows triggered by a data permit or data request and is enforced through technical controls implemented within the CY-EHDS-2nd infrastructure. All FRs apply exclusively to operations inside the ISPE and are thoroughly presented in Table 8.

Table 8: CY-EHDS-2nd ISPE FRs

FRs	**ISPE-FR1**
Requirement	Secure Dataset Ingestion
Involved Actors	Data Holders, NeHA Operators
Requirement Features	- Data access–scoped SFTP drop zone
	- logical isolation
	- ACL-based access control
	- Data permit or data requestID binding
Detailed Description	Each ISPE instance must receive datasets from data holders through a SFTP channel that is isolated per data permit or request. All dataset uploads must be traceable to the specific data holder and access request ID, and logged centrally.
Use Case(s)	**ISPE-UC1: Upload of Raw Dataset by Data Holder** A data holder receives notification to upload datasets into a scoped SFTP drop zone. Access is limited to their credentials and timeframe. **ISPE-UC2: Upload of Raw Dataset by Data Holder** Traceable File Movement Linked to Permit ID: All uploads must be tagged and logged using the data access ID, ensuring traceability and non-repudiation.

FR	ISPE-FR2
Requirement	Operator Authentication and Access Control
Involved Actors	ISPE Operators
Requirement Features	- CY Login + mTLS authentication
	- VM-scoped access
	- no external exposure
Detailed Description	Access to the ISPE VMs by designated ISPE Operators is strictly controlled. Authentication is managed by the CY-EHDS-2nd CPL through the national CY Login service, supplemented by mandatory mTLS client certificate validation for operators. Following successful authentication and high-level role validation (i.e. confirming the user is an ' ISPE Operator') by the CPL, operators are granted access to the relevant ISPE environment(s). Within the ISPE, access is further scoped to specific VMs based on operational needs related to active data permits or requests. All such access is logged centrally via the CPL and the shared observability stack.
Use Case(s)	ISPE-UC3: Operator Login to Permit-Scoped VM: Only authenticated operators with explicit rights can enter the SPE for processing actions. ISPE-UC4: Enforcing Isolation from Unauthorised Sessions: All access attempts are validated against access scopes. External users are explicitly excluded.
FR	**ISPE-FR3**
Requirement	**Data Access–Scoped Processing Only**
Involved Actors	ISPE Operator
Requirement Features	- Scope-bound execution
	- Authorised data operations
	- Runtime traceability
Detailed Description	All processing within the ISPE must strictly comply with the access parameters defined in the approved data permit or request. The SPE must enable the use of authorised data preparation and transformation techniques including pseudonymisation, aggregation, filtering, data linking,

	formatting, and cleaning. No data may be transformed or accessed beyond what is explicitly authorised. All actions must be traceable and bounded by the permit configuration.
Use Cases	**I**SPE-UC5: Executing Processing Within Permit Scope: Operators carry out data transformations using the allowed tools and configurations as defined in the data access decision. All actions are monitored and limited to the approved purpose.
FR	**ISPE-FR4**
Requirement	Script Vault and Formula Retention
Involved Actors	ISPE Operator, NeHA Governance
Requirement Features	- Optional on request
	- Permit-linked storage
	- Internal-only access
Detailed Description	At the request of the data user, the processing scripts or formulas used in the ISPE must be retained in a secure Script Vault. Each script is tagged to its corresponding data access ID and stored for reuse or reproducibility.
Use Cases	**ISPE-UC6: Retaining Data Processing Scripts by Permit ID**: Operators upload script artifacts into the internal vault as documentation of transformations used under each access case.
FR	**ISPE-FR5**
Requirement	Result Review and Controlled Release
Involved Actors	ISPE Operator
Requirement Features	- Manual review
	- Dual result flows (dataset/statistics)
	- No raw data export
	- Closure triggers upon delivery

Detailed Description	All output generated within the ISPE must be manually reviewed by the operator. For permits, datasets are transferred to the ESPE. For requests, statistical outputs are sent via secure email. No raw data may leave the ISPE.
Use Cases	**ISPE-UC7: Internal Transfer to ESPE for Data Permits:** Prepared pseudonymised datasets are made available to the data user's ESPE. **ISPE-UC8: Statistical Result Email for Data Requests:** Aggregated statistical results are reviewed and sent securely to the requester via email.
FR	**ISPE-FR6**
Requirement	Centralised Audit Logging
Involved Actors	ISPE Operator, NeHA Audit Infrastructure
Requirement Features	- Permit/request ID binding
	- Time-stamped logging
	- Immutable records
Detailed Description	All ISPE operations must be logged in the central audit system, including access, processing actions, and file transfers. Each log entry must be tied to a data access ID and retained for inspection in accordance with EHDS Article 73(3).
Use Cases	**ISPE-UC8: Traceable File Movement Linked to Permit ID :** All log records must match the access lifecycle and be immutable for review. **ISPE-UC9: Enforcing Isolation from Unauthorised Sessions:** Failed or blocked access attempts are also logged as part of audit coverage.
FR	**ISPE-FR7**
Requirement	Data Access–Scoped VM Lifecycle Enforcement
Involved Actors	NeHA Infrastructure Team
Requirement Features	- Permit/request-linked VM ID
	- lifecycle trigger
	- Maximum duration six months after data permit expiration or revocation
Detailed Description	Each ISPE VM must be provisioned per data access decision and decommissioned no later than six months after its expiry, in accordance with EHDS Article 68(12). Temporary storage must be purged securely.
Use Cases	**ISPE-UC10: Traceable File Movement Linked to Permit ID:** Final logs confirm permit closure and trigger VM shutdown workflow. **ISPE-UC11: Enforcing Isolation from Unauthorised Sessions:** VM is deleted and cannot be accessed beyond its lifetime.

5.4 Non-Functional Requirements

The ISPE must operate under a set of strict NFRs that ensure the confidentiality, integrity, traceability and auditability of all operations conducted within it. These constraints apply to the infrastructure, access control model, system behaviour and overall compliance mechanisms that govern the functioning of the ISPE.

It is important to note that this section includes only the NFRs that are specific to the ISPE, either because they are implemented differently or exclusively within this environment. Requirements that are shared between the Internal and ESPEs are addressed separately in Chapter 7, which consolidates all system-wide technical and security constraints (Table **9**).

Table 9: CY-EHDS-2nd ISPE NFRs

NFR	**ISPE-NFR1**
Requirement	Infrastructure Security
Description	ISPEs must be deployed on isolated network zones within NeHA infrastructure. No direct internet connectivity is allowed to or from any ISPE VM. The infrastructure must enforce firewall segmentation, OS-level hardening, and role-based deployment access.
Measure/Compliance indicator	- Network isolation policy - Firewall rules audit - System hardening compliance reports
NFR	**ISPE-NFR2**
Requirement	Session Integrity and Timeout
Description	ISPE operator sessions must time out after 15 minutes of inactivity. Max session duration is limited to 1 hour. CY Login with client certificate is required per session. Sessions are isolated per operator and data access ID.
Measure/Compliance indicator	- CY Login session policy - Session audit logs - Inactivity timeout simulation results
NFR	**ISPE-NFR3**
Requirement	Data Permit-Bound VM Lifecycle
Description	Each ISPE instance must be provisioned per data permit or request and deleted no later than six months after permit expiry, in accordance with Article 68(12) of the EHDS Regulation.
Measure/Compliance indicator	- VM metadata tagged by permit ID - Expiry-based lifecycle triggers - Destruction logs archived
NFR	**ISPE-NFR4**

Requirement	Processing Auditability
Description	All actions performed inside the ISPE, including dataset loading, transformation, file movements, and script executions, must be logged in a tamper-evident, central audit system. Each log entry must reference the associated data access ID and operator ID.
Measure/Compliance indicator	- Immutable log infrastructure - Signed entries per event - Log retention policy (per data permit)
NFR	**ISPE-NFR5**
Requirement	Script Vault and Execution Traceability
Description	When requested by the data user, all scripts used in dataset preparation must be retained in a secure internal Script Vault. Scripts must be tagged with metadata including operator ID, permit ID, date and version.
Detailed Description	Before transferring a dataset to the ESPE or finalising a statistical response, the ISPE configuration (tools used, scripts, operator roles, access status) must be verifiable for audit.
Measure/Compliance indicator	- Vault encryption - Version control system logs - Retention and access audit logs
NFR	**ISPE-NFR6**
Requirement	Monitoring and Resource Oversight
Description	ISPE infrastructure must support real-time monitoring of CPU, memory, and disk usage. Resource alerts must be configured to avoid overload and performance bottlenecks during processing of large health datasets.
Measure/Compliance indicator	- Threshold-based alerts - Monthly utilisation reports
NFR	**ISPE-NFR7**
Requirement	Intra-SPE Access Isolation
Description	Each ISPE instance must guarantee that data accessed within a session is strictly scoped to the specific data access ID. No cross-permit or cross-session data visibility is allowed.
Measure/Compliance indicator	- VM access policy audit - Isolation test reports - Access attempt logs per session ID

5.5 Technical Specifications

This section provides the technical specifications of the ISPE as implemented under CY-EHDS-2nd. The specifications reflect how the previously defined requirements are translated into infrastructure, interfaces, tooling, and runtime behaviours.

All components of the ISPE are hosted and operated by NeHA on secure national infrastructure and are designed to ensure full compliance with the security, privacy, and auditability obligations defined in the EHDS regulation, particularly Article 73. The following subsections describe the key architectural, interface, operational, and security parameters that govern the ISPE.

In the CY-EHDS-2nd architecture, each ISPE processing session is provisioned in a dedicated VM scoped to a single data permit or data request ensuring strict isolation, complete traceability and clean lifecycle closure for each data access case. Once processing is completed and outputs are delivered, the VM is either archived for audit or securely deleted, depending on the data permit and data request retention policy.

5.5.1 Operational Environment Specs

Table 10: CY-EHDS-2nd ISPE Operational Environment

ID	Environment Constraint
ITS-OE1	ISPE VMs run on virtual infrastructure managed by NeHA, deployed in private cloud or on-prem cluster.
ITS-OE2	VMs are managed by NeHA DevSecOps pipelines and provisioned through infrastructure-as-code (e.g., Terraform).
ITS-OE3	Each VM must be tagged with permit/request ID and destroyed no later than six months after its expiry.

5.5.2 Interfaces and Data Ingestion Specs

Table 11: CY-EHDS-2nd ISPE Interfaces & Data Ingestion

ID	Interface	Description
ITS-IF1	SFTP Ingestion Interface	Receives datasets from data holders into permit/request-specific isolated directories.
ITS-IF2	Operator Access Interface	Authenticated via CY Login (eID) and mTLS; authorisation scoped to specific VMs.
ITS-IF3	Audit Logging Interface	Sends structured logs to central immutable log store, per the CPL-defined API.
ITS-IF4	Output Transfer Interface	Transfers prepared datasets to ESPE or sends statistical results via internal NeHA email.
ITS-IF5	Monitoring Interface	Connects to shared monitoring agent to expose resource usage metrics and alerts.

5.5.3 Quality Specs

Table 12: CY-EHDS-2nd ISPE Quality

ID	Requirement	Specification
ITS-QR1	Availability	ISPE must be provisioned within 4 hours of data permit approval.
ITS-QR2	Performance	Must support concurrent data processing up to 2GB per session without resource exhaustion.
ITS-QR3	Security Isolation	Each VM must be deployed in a network-isolated namespace with no internet access.
ITS-QR4	Session Control	Sessions must time out after 15 minutes of inactivity. Max session length = 1 hour.

ITS-QR5	Logging Integrity	All audit logs must be timestamped, signed, and stored in tamper-evident storage.
ITS-QR6	Script Traceability	Vaulted scripts must include operator ID, permit ID, and hash of execution version.

5.5.4 *Design Constraints Spec*

Table 13: CY-EHDS-2nd ISPE Output Preparation & Delivery

ID	Constraint
ITS-DC1	Outbound internet access is blocked by default for all ISPE VMs.
ITS-DC2	No shared storage is allowed across SPE instances.
ITS-DC3	SPEs must rely only on free, offline-compatible software tools unless specifically approved.
ITS-DC4	All operator sessions must be linked to a logged CY Login identity and permit ID.

5.5.5 *Logging Integration Specs*

Table 14: CY-EHDS-2nd ISPE Logging Integration

ID	Specification
ITS-LG1	The ISPE must emit structured, timestamped logs for all user and system actions, including: user login, dataset retrieval, script execution, data transformation, and file export operations.
ITS-LG2	All logs must be forwarded to the central audit logging infrastructure governed by CPSS4 (Logging, Monitoring, and Audit).
ITS-LG3	Log entries must include: operator ID, permit or request ID, timestamp, action type, and success/failure result.
ITS-LG4	Logs must be retained for a the period defined in data permit or data request and protected against tampering using write-once, immutable storage.

5.5.6 *Monitoring and Observability Specs*

Table 15: CY-EHDS-2nd ISPE Monitoring and Observability

ID	Specification
ITS-MN1	Each ISPE VM must expose system-level metrics (CPU usage, memory consumption, disk I/O, and active session count) to the central observability stack used in the national infrastructure.
ITS-MN2	Alerts must be generated when predefined thresholds are breached (e.g., CPU > 90% for >10 mins).
ITS-MN3	Metrics must be tagged by VM and permit/request ID, and retained for 12 months to support operational tuning and incident response.

5.5.7 *Security and Operator* **Workstation** *Constraints Specs*

Table 16: CY-EHDS-2nd ISPE Security and Operator Workstation Constraints

ID	Specification
ITS-OP1	Operator access is limited to pre-approved tools installed within the ISPE VM. No installation of third-party software or plugins is allowed.
ITS-OP2	Only offline-compatible, pre-validated tools are installed, including: R (CLI), Python, LibreOffice (offline), shell utilities (e.g. awk, jq), and data transformation scripts.

ITS-OP3	Operator access is read/write only to scoped working directories within the VM and cannot access system directories or other user sessions.
ITS-OP4	No file may be exported from the ISPE to an external device or system unless explicitly approved through the defined output handling process.

6 EXTERNAL SECURE PROCESSING ENVIRONMENT

The ESPE is a core component of the CY-EHDS-2nd architecture dedicated to data analysis by authorised data users. Managed and hosted by the HDAB (NeHA) on secure national infrastructure, it provides a virtualized, isolated workspace for data users who have obtained an approved data permit. Within this environment, a data user can access and analyse a prepared health dataset under strict security and privacy controls. The ESPE is provisioned on a per data permit basis, meaning a separate secure workspace is set up for each specific data permit and its named authorised data user(s).

In essence, the ESPE functions as a "safe data analysis room" in cyberspace. It hosts only the pseudonymised dataset prepared for that permit (no raw identifiable data), along with a suite of analytical tools. The environment is fully sandboxed: it has no connection to the open internet or external devices, and it prevents any unapproved data extraction. Authorised data users log in through mature authentication including a secure national login system (CY Login with 2FA) and a client certificate to enter this workspace. Once inside, they can perform computations, statistical analysis, or machine learning on the dataset, but cannot copy, download, or remove any data directly. All actions are confined within the SPE and are subject to monitoring and auditing. When the analysis is complete, the user's results (e.g. statistical summaries, charts, or trained models) can be exported in a controlled manner, after passing compliance checks to ensure no sensitive data is leaving the environment.

The ESPE is designed to meet the EHDS regulation requirements for secure data processing. It ensures that data analysis for secondary use (research, policymaking, etc.) occurs under high security and privacy safeguards. By operating this environment, the HDAB (NeHA) enables external data users to derive insights from health data without ever exposing the underlying sensitive data outside the national secure infrastructure. In summary, the ESPE is a secure virtual lab for authorised individuals to analyse health datasets under supervision, offering robust computing resources, built-in analysis software, and stringent protections that align with national and EU data governance standards.

6.1 Actors and Interfaces

The ESPE involves a focused set of actors, each with defined roles and access methods. As with the ISPE, all interactions are tightly governed by the conditions of the data permit and by the security policies established by the HDAB (NeHA). Table **17** presents the key actors of the ESPE as defined in *D5.1 Annex D: Common Actor Definitions – CY-EHDS-2nd (v1.0)*, while Table **18** outlines the technical interfaces through which these actors interact with the ESPE. All network communication with the ESPE is through secure, controlled channels while there is no open network exposure. Data confidentiality and user accountability are maintained by authenticating every user action and by logging all operations in a central audit system.

Field Code Changed

Field Code Changed

Table 17: CY-EHDS-2nd ESPE Actors as defined in *D5.1 Annex D: Common Actor Definitions – CY-EHDS-2nd (v1.0)*

Actor No.	Actor

A2	Data User
A5	Data Permit Manager
A11	External SPE Operator
A31	HDAB Business Owner / Solution Provider

Table 18: Table 7: CY-EHDS-2nd ESPE Interfaces

Actor	System Interface Used	Interface Description
ISPE Operator	ISPE push mechanism / configuration trigger (NeHA-controlled)	The ESPE Operator receives the prepared dataset from the ISPE once processing is complete and validated. They then provision the ESPE VM and load the dataset for the permitted data user(s). This workflow is manual, controlled, and logged.
ESPE Operator	Remote desktop to permit-scoped environment management console	SPE Operators provision and manage each ESPE environment. They apply user-specific configurations, enforce permit-based access conditions, and suspend or deactivate environments once the permit expires. All actions are centrally logged.
Data User	Remote desktop to ESPE envidonrment via CY Login + client certificate	The named user accesses the provisioned SPE instance using strong authentication (CY Login + mTLS). Sessions are sandboxed, and users have access only to the tools and datasets explicitly authorised in the data permit.
Audit & Compliance Officer	Read-only access to log store and session reports	This role interfaces with the central logging and monitoring systems to inspect access logs, system events, and session activity reports for compliance verification and security review.
NeHA (Platform Monitoring)	Central observability and alerting stack	ESPE environments expose system metrics (CPU, memory, session uptime) to the shared monitoring system. Alerts are raised if predefined thresholds are violated. Logs and metrics are tagged with the data permit ID and user ID.

6.2 ESPE Hosting and Operator Model

In the framework of CY-EHDS-2nd, the ESPE infrastructure is hosted and operated entirely by NeHA. Each ESPE is instantiated as a dedicated VM, provisioned per approved data permit, and configured exclusively for the named data users listed in that permit. These environments are deployed on NeHA national infrastructure, ensuring full jurisdictional control and compliance with EHDS and GDPR provisions.

NeHA currently acts as both the HDAB and the sole SPE provider in Cyprus. As such, it is responsible for:

- Hosting and maintaining the physical and virtual infrastructures
- Provisioning and terminating ESPE instances based on permit lifecycles
- Enforcing access control, resource monitoring, and isolation policies
- Reviewing any requests for result extraction in accordance with the permit scopes

The ESPE Operator, a technical role designated by NeHA, performs the provisioning, configuration, and shutdown of each SPE instance. The operator applies the rules defined in the data permit, including:

- Identified users (data users)sPermitted datasets and duration

- Allowed software tools
- Extraction policy (results only, no raw data)

ESPE instances are ephemeral, tightly scoped, and destroyed no later than six months after the expiry of the permit, in accordance with EHDS Article 68(12).

As the national infrastructure matures and other accredited data users or SPE providers are authorised in the future, the ESPE may evolve into a multi-tenant model. However, for now, NeHA is the only SPE provider, and all hosting responsibilities are centralised.

6.3 High-Level Architecture

This section describes the architectural components and operational layout of each ESPE instance as provisioned per data permit, following the validated model of the CY-EHDS-2nd national infrastructure. Each ESPE is instantiated as a virtualised analysis environment, scoped to the specific data permit and tightly bound to the named data users approved by NeHA. The architecture ensures strong isolation, compliance with security and access constraints, and full traceability of user activities. Table **19** presents the core components of each ESPE instance.

Field Code Changed

Table 19: CY-EHDS-2nd ESPE Core Components

Component	Description
VM	Dedicated runtime environment deployed per data permit. Hosted within NeHA infrastructure (private cloud/on-prem). Destroyed automatically after permit expiry + 6 months.
Data Access Control Layer	Applies RBAC and session constraints. Grants access only to authorised users via CY Login + client certificate. Access is isolated per user and permit.
Pre-loaded Dataset (Input)	The prepared dataset (pseudonymised and approved) is pushed from the ISPE. The dataset is mounted as read-only.
Analysis Tools Layer	Includes only offline-compatible, pre-approved software (e.g. RStudio Server, Python, JupyterLab, STATA if licensed). Installed in read-only containers.
Result Output Interface	Allows export of analysis results (e.g. graphs, tables) under the terms of the permit. All extraction actions are logged and reviewed.
Session & File Logging Agent	Logs user login, session duration, command execution, file reads/writes, and output exports. Logs are tagged with permit and user ID and sent to the central log store.
Resource Monitoring Agent	Exposes VM metrics (CPU, memory, session uptime) to the central monitoring system, enabling real-time alerts.

6.4 ESPE Lifecycle

Each ESPE instance follows a strict, traceable lifecycle scoped to a specific approved data permit. It is configured, accessed, and decommissioned according to technical and legal rules enforced by NeHA under the CY-EHDS-2nd infrastructure.

The following lifecycle steps are implemented per permit:

1. Permit Approval and Dispatch

The ESPE lifecycle is initiated following the formal approval of a data permit for secondary use within the CY-EHDS-2nd DAAMs (WP5). The HDAB Data Permit Manager extracts the critical operational parameters from the data permit in DAAMs. These parameters, including the unique permit ID, list of authorized natural persons (Data Users), specified datasets, permit validity period, approved analytical tool profile, and data extraction/output policies, are then securely communicated to the designated NeHA ESPE Operator(s). This communication currently occurs via a defined internal procedure (e.g. encrypted email with a standardized template), forming the authoritative instruction for provisioning the ESPE instance.

2. ESPE Provisioning

Upon receiving the permit parameters, the NeHA ESPE Operator provisions a dedicated and isolated VM for the specific data permit. This VM is:

- Tagged with the unique Permit ID.
- Configured strictly according to the permit parameters, which includes:
    - Securely loading the approved, prepared (typically pseudonymised) dataset received from the ISPE. This dataset is mounted as read-only for the Data User.
    - Preloading only the whitelisted analytical tools (e.g. RStudio Server, Python, JupyterLab) authorised by the permit.
    - Enforcing all technical security policies, such as network isolation (no internet access), specific RBAC configurations for the permitted users, and session isolation measures. Once the ESPE VM is provisioned and validated by the operator, NeHA informs the authorized Data User(s) listed in the permit (e.g. via secure email or a notification from the CPL system in future iterations) that their secure analysis workspace is ready for access. The environment remains inaccessible until successful user authentication via the CPL.

3. User Authentication and Access

Authorized Data Users access their provisioned ESPE VM through the CY-EHDS-2nd CPL, which manages authentication. This process requires:

- Authentication via the national CY Login service.
- Possession and validation of a mTLS client certificate issued to the authorised individual. Upon successful authentication and high-level role validation by the CPL, the system verifies that the user is explicitly listed on the active data permit associated with the requested SPE VM. Only then is access granted to the specific remote desktop or secure web interface of their dedicated SPE VM. Each session is uniquely identified and tied to both the User ID (from CPL) and the Permit ID. All

access attempts (successful or failed) and session initiation details are logged in the central CY-EHDS-2nd observability stack.

4. Analysis and Data Use

Inside the ESPE:

- The dataset is available in read-only format.
- Users may create local, in-memory subsets for analysis but cannot modify the source.
- Only approved tools are usable (offline-compatible).
- No uploads, internet access, or external connections are permitted.
- System-level controls block disallowed actions (e.g. clipboard copy, browser launch).

Collaborative analysis is supported only if multiple users are explicitly listed on the same permit. Each user logs in independently, and all actions are individually logged.

5. Monitoring and Oversight

All activities within the ESPE are subject to monitoring and oversight by NeHA:

- **Activity Logging:** All Data User actions (logins, script execution, file access, tool usage, export requests, session termination) are comprehensively logged with identifiable details (User ID, Permit ID, timestamp, action) and streamed to the central CY-EHDS-2nd observability stack.
- **System Metrics & Alerts:** The ESPE VM emits system metrics (CPU, memory, session uptime) to the central observability stack. NeHA operational teams monitor these metrics and configure alerts for abnormal behavior, potential security incidents (e.g., repeated failed export attempts, resource exhaustion), or unauthorised access attempts.
- **Session Management:** User sessions are automatically locked after a defined period of inactivity (e.g. 15 minutes) and expire after a maximum duration (e.g. 1 hour, unless extended per policy), enforced by the SPE environment in conjunction with CPL session policies where applicable. Direct communication with Data Users regarding support or policy queries is handled by NeHA through secure channels external to the SPE VM.

6. Output Export Request

When users wish to extract results:

- Files are moved to a dedicated export review zone within the SPE.
- The system blocks direct user export and notifies the operator.
- Scripts, figures, or tables may be included, but all must undergo review.
- Every request is logged, including file metadata and user ID.

7. Output Review and Release

When a Data User requests to export analytical results, the designated files are moved to a secure export review zone within the SPE, and direct user download is blocked. The NeHA ESPE Operator is notified and conducts a thorough review to:

- Verify that the requested outputs (e.g. statistical summaries, aggregated tables, de-identified charts) comply with the data export policies defined in the data permit.
- Ensure that the outputs contain only non-personal, aggregated, or appropriately de-identified data, with no residual personal data or information that could lead to the re-identification of individuals, in strict compliance with EHDS Article 73(1)(b) and 73(2). Non-compliant outputs are rejected, and feedback is provided to the Data User. Approved, compliant results are released to the Data User via a NeHA-defined secure mechanism (e.g. secure download link via CPL, encrypted email). All review decisions, timestamps and details of released outputs are logged.

8. Expiry and Decommissioning

Upon the expiration or termination of the associated data permit, the ESPE VM enters the decommissioning phase, strictly adhering to EHDS Article 68(12) and the general operational lifecycle (Section 4.5):

- User access to the SPE VM is immediately revoked.
- The ESPE VM and all associated data (including the prepared dataset and any temporary user work files) are securely deleted no later than six months after the data permit's expiry date. The deletion process is logged.
- Computational scripts or processing logic (formulas) may be retained by NeHA in the secure 'Script Vault' if requested by the Data User and approved under NeHA governance, as per EHDS Article 68(12).
- Final audit logs pertaining to the SPE VM's operation are archived within the central CY-EHDS-2nd observability stack according to defined retention policies. The lifecycle for that permit-specific ESPE is then formally closed.

6.5 Functional Requirements

To support the above workflow and objectives, the ESPE must fulfil several FRS. These are the key capabilities or functions that the system should provide to ensure secure, convenient, and compliant data analysis for external users. Each requirement is numbered (continuing from the ISPE requirements) and includes a brief description of the function, the actors involved, and the main features or criteria of that requirement (Table **20**).

Table 20: ESPE FRs Overview

FR	**ESPE-FR1**
Requirement	**Secure Authentication and Access Enforcement**
Involved Actors	Data User, ESPE Operator, CY Login IAM
Requirement Features	- CY Login + client certificate (mTLS) - Named-user validation against data permit - Session timeout - Single session per user
Detailed Description	Data User access to the ESPE is stringently managed. Initial authentication is performed by the CY-EHDS-2nd CPL using the national CY Login service, coupled with mandatory mTLS client certificate validation. Following successful CPL authentication and validation of the Data User role, the CPL facilitates routing to the SPE environment.

	Access to a specific ESPE VM is then granted only if the authenticated Data User is explicitly named on the active data permit associated with that VM. This permit-specific authorisation (i.e. linking the CPL-authenticated user to a particular VM based on permit details) is currently applied by the ESPE Operator during the VM provisioning phase, based on instructions from the HDAB Data Permit Manager who interprets the approved permit from DAAMs. Sessions are tied to the user ID and the unique data permit ID. All access attempts and session activities are centrally logged via the CPL and the shared observability stack
Use Cases	**ESPE-UC1**: A named user logs into the ESPE for the first time using CY Login and client certificate. **ESPE-UC2**: A login attempt by a non-permitted individual is denied and logged. **ESPE-UC3**: A session is automatically locked after 15 minutes of inactivity.
FR	**ESPE-FR2**
Requirement	Environment Provisioning and Permit-Based Configuration
Involved Actors	ESPE Operator, Data Permit Manager
Requirement Features	- VM instantiation - Permit-scoped dataset and tool configuration - Permit tagging and metadata application
Detailed Description	Upon permit approval, the ESPE Operator must provision a new, isolated VM tagged with the permit ID. The environment must include the preapproved dataset (read-only) and only the tools permitted under the data permit. Provisioning must ensure compliance with permit-specific parameters (users, duration, tools).
Use Cases	**ESPE-UC4**: An SPE Operator provisions a new VM and configures it for a 6-month permit. **ESPE-UC5**: A permit with two users and an export restriction triggers the creation of a collaborative, read-only dataset VM with shared access enabled.
FR	**ESPE-FR3**
Requirement	Controlled Dataset Access and Usage
Involved Actors	Data User, ESPE Operator
Requirement Features	- Dataset mounted as read-only - Access scoped to local SPE memory - No modification or re-export of raw data
Detailed Description	The ESPE must provide access to the dataset as read-only. Users can create in-memory views or temporary subsets but cannot export or alter the original dataset. The mount must be immutable and logged.
Use Cases	**ESPE-UC6**: A user runs a statistical query on the dataset and saves intermediate results in local session memory. **ESPE-UC7**: An attempt to move the dataset to an export folder is blocked and flagged.
FR	**ESPE-FR4**
Requirement	Approved Tool Execution Control
Involved Actors	Data User, ESPE Operator
Requirement Features	- Preinstalled tool whitelist- Session container security- Execution sandboxing
Detailed Description	Only tools explicitly listed in the permit must be made available inside the ESPE (e.g. RStudio, Python, STATA if licensed). Unauthorised software or commands (e.g. opening browsers, file transfers) must be blocked at runtime and logged.

Use Cases	**ESPE-UC8**: The user launches JupyterLab for analysis as allowed by the permit. **ESPE-UC9**: A script attempting to launch an unapproved web browser is blocked.
FR	**ESPE-FR5**
Requirement	Output Export Request and Review
Involved Actors	Data User, ESPE Operator
Requirement Features	- Export tagging interface - File review zone - Operator approval workflow
Detailed Description	The user must submit output files (e.g. graphs, scripts, tables) for approval via a designated export interface. The files are held for review by NeHA. No file may be extracted until operator validation is complete. All requests and approvals must be logged.
Use Cases	**ESPE-UC10**: A user tags two statistical tables and a plot for export. **ESPE-UC11**: The SPE Operator reviews and approves only one table, rejecting the others for granularity.
FR	**ESPE-FR6**
Requirement	Collaborative User Session Management
Involved Actors	Multiple Data Users, ESPE Operator
Requirement Features	- Shared workspace instance- Individual login audit - Scoped resource access
Detailed Description	If a data permit authorises multiple users, the ESPE must support collaboration via shared access. All user actions must be attributed and logged. Collaborative tools must be confined within the SPE environment.
Use Cases	**ESPE-UC12**: Two users access the same SPE instance and co-author an analysis notebook. **ESPE-UC13**: One user mistakenly attempts to access the other's files and is denied.
FR	**ESPE-FR7**
Requirement	Lifecycle Termination and Data Erasure
Involved Actors	ESPE Operator, Platform Monitoring
Requirement Features	- Time-based expiration - Automated teardown - Destruction logging
Detailed Description	Upon permit expiry, the SPE must be suspended and permanently deleted no later than six months after the end date of related data permit. Destruction must be logged, and user access revoked. No residual datasets or files must persist.
Use Cases	**ESPE-UC14**: A VM is auto-suspended at permit expiry and locked for 6-month retention. **ESPE-UC15**: After 6 months, the SPE is destroyed, and destruction is logged in the central audit system.

6.6 Non-Functional Requirements

The ESPE must meet strict NFRs to ensure it operates securely, predictably, and within the boundaries of the approved data permit. These requirements are derived from the system's design goals under CY-EHDS-2nd, as well as from EHDS Article 73 and GDPR accountability obligations. Shared NFRs that apply to both SPE types are presented in Chapter 7. This section includes only External-SPE-specific constraints (Table **21**).

Table 21: ESPE NFRs Overview

Code	**ESPE-NFR1**
Requirement	Session Response and Performance Integrity
Description	The ESPE must maintain interactive performance during analysis sessions. Each user session must respond to commands (e.g. code execution, tool launch) within 3 seconds under normal load.
Measure/Compliance Indicator	- Monitoring data confirms response time below threshold 95% of the time- alerts trigger on CPU saturation or memory swap overflow.
Code	**ESPE-NFR2**
Requirement	User Access Availability
Description	The ESPE must be available to the data user throughout the approved permit window, with a target uptime of 99% during permitted hours.
Measure/Compliance Indicator	- Availability logs -Automatic VM recovery on failure -Permitted access time enforced via permit-linked timers.
Code	**ESPE-NFR3**
Requirement	Permit-Scoped VM Lifecycle Enforcement
Description	Each SPE VM must be instantiated only after permit approval and destroyed no later than six months after permit expiry.
Measure/Compliance Indicator	- Orchestration logs show exact creation and deletion time linked to the permit ID - VM metadata enforces expiry-based auto-decommissioning
Code	**ESPE-NFR4**
Requirement	Access Control and Isolation
Description	Each SPE instance must be accessible only to named users using CY Login and client certificate (mTLS), with strict RBAC applied. Users must be isolated from each other unless explicitly permitted for collaborative access.

Measure/Compliance Indicator	- Authentication logs - Session UUIDs - Denial events for unauthorised login - Isolation policy configuration for each VM instance
Code	**ESPE-NFR5**
Requirement	Output Protection and Review Process
Description	No files or results may exit the ESPE without operator review. All exports must be routed through a gated review queue.
Measure/Compliance Indicator	- Export logs show: file ID, request timestamp, user ID, operator decision, delivery trace. Denied or modified exports are retained.
Code	**ESPE-NFR6**
Requirement	Tool Whitelisting and Execution Control
Description	Only tools pre-approved in the data permit may be available in the ESPE. Runtime policies must block disallowed software.
Measure/Compliance Indicator	-Whitelist check during container boot -Denied process logs -Checksum enforcement of installed binaries
Code	**ESPE-NFR7**
Requirement	Audit Logging and Retention
Description	All user actions (login, file access, script execution, export request) must be logged with timestamps and permit reference ID. Logs must be retained for at least 12 months post VM deletion.
Measure/Compliance Indicator	- Audit trail completeness reports - Log immutability status - Archival status tagged to VM lifecycle
Code	**ESPE-NFR8**
Requirement	Inactivity Timeout and Auto-Lock

Description	SPE sessions must auto-lock after 15 minutes of user inactivity and auto-expire after 1 hour of total session duration unless extended manually.
Measure/Compliance Indicator	- Session timeout events in logs -Lock screens triggered by timer -Session duration monitored via heartbeat signals
Code	**ESPE-NFR9**
Requirement	Resource Monitoring and Threshold Alerting
Description	The ESPE must emit metrics to the central observability system. Thresholds must be defined for CPU, memory, disk I/O, and session duration.
Measure/Compliance Indicator	- Metrics pushed every 60s - Alerts configured for ≥90% CPU or ≥80% RAM- operator notified on breach
Code	**ESPE-NFR10**
Requirement	Usability and Environment Readiness
Description	Each ESPE instance must be fully usable without requiring manual installation or setup by the data user. Tools, data, and workspace must be available on first login.
Measure/Compliance Indicator	- User environment health check script -Zero-error login confirmation -Tool path verification before session start

6.7 Technical Specifications

This section provides the technical specifications of the ESPE. The specifications detail how the ESPE's requirements are realised in terms of infrastructure, interfaces, analytical tooling, and operational security. All components of the ESPE are hosted and managed by NeHA on secure national infrastructure, designed to fulfil the stringent security, privacy, and auditability obligations of the EHDS regulation (notably Article 73). The following subsections describe the key architectural, interface, toolset, and security parameters governing the ESPE.

6.7.1 Virtual Environment and Architecture

This subsection defines the technical structure and configuration of the VM that hosts each ESPE instance under a specific data permit. Each environment is created as a secure, isolated, and ephemeral workspace scoped to the terms of that permit (Table **22**).

Table 22: NFR - ESPE - Virtual Environment and Architecture

Code	Component	Specification
ETS-VE1	**Virtualisation Platform**	Hosted on NeHA-managed national infrastructure. VM instantiated using hardened templates managed under secure CI/CD pipeline.
ETS-VE2	**VM Isolation**	Each SPE instance is deployed in a dedicated network and namespace. No connectivity between SPE VMs is allowed. Only internal NeHA-managed endpoints are reachable.
ETS-VE3	**Operating System (Guest)**	Hardened Linux image with preinstalled tools, firewall rules, host-level anti-tamper controls.
ETS-VE4	**Data Volume Mounts**	Input dataset mounted as read-only volume. Export folder mounted as write-only, permission-controlled volume visible only to operator for review.
ETS-VE5	**Storage Encryption**	All volumes are encrypted at rest (AES-256), bound to the VM instance lifecycle. No volume is accessible after decommissioning.
ETS-VE6	**Session Environment**	User environment delivered via remote desktop (e.g. XRDP, Guacamole) or browser-based interface. Clipboard, copy-paste, and network access are disabled.
ETS-VE7	**User Work Directory**	Private, non-persistent scratch space within the SPE VM. Not backed up. Destroyed after session or SPE decommissioning.
ETS-VE8	**Session Identity Binding**	User workspace tied to their CY Login identifier and permit reference. Only one active session per user per SPE is permitted.
ETS-VE9	**Containerised Tool Layer**	Tools (e.g. RStudio, Python, JupyterLab) are installed in read-only containers using digitally signed builds. No user installation allowed inside VM.

6.7.2 Access & Authentication Model

This subsection defines the technical mechanisms for authenticating authorised users into the ESPE environment and for ensuring access aligns strictly with the data permit terms (Table **23**).

Table 23: NFR - ESPE - Access & Authentication Model

Code	Component	Specification
ETS-AM1	**Authentication Method**	Users must authenticate using CY Login (national eID federation) with mandatory mTLS client certificate issued to their institution or personal identity.
ETS-AM2	**Permit Binding**	The SPE environment is bound to the permit ID, and access is granted only if the CY Login identity matches one of the authorised users in the permit metadata.
ETS-AM3	**Session Enforcement**	Only one active session per user per SPE is allowed. Sessions are non-transferable. New sessions terminate previous ones automatically.
ETS-AM4	**Session Timeout**	Sessions auto-lock after 15 minutes of inactivity. Users are logged out after 1 hour of continuous runtime unless extended by operator policy.
ETS-AM5	**Access Logging**	Every login, logout, session start, failure, timeout, and extension is logged centrally. Logs include user ID, permit ID, session UUID, IP origin, and timestamp.
ETS-AM6	**Access Denial Policy**	Failed authentication attempts due to invalid certificates, expired sessions, or unauthorised identity mismatches are immediately denied and logged.

ETS-AM7	**Operator Access (Administrative)**	ESPE Operators may access the VM for maintenance via secure internal VPN and role-based SSH key access. All such sessions are tagged as operator and logged separately.

6.7.3 Tooling Environment

This subsection defines the analytical software stack available to users inside each ESPE, including restrictions, installation policies, and execution constraints (Table **24**).

Table 24: NFR - ESPE - Tooling Environment

Code	Component	Specification
ETS-TE1	**Tool Preinstallation**	The SPE VM is preconfigured with approved analytical tools defined in the permit, using NeHA-validated and signed container images. No internet is used during provisioning.
ETS-TE2	**Permitted Tools**	Examples include: RStudio Server, JupyterLab (Python/R), LibreOffice, STATA (if licensed), VS Code (offline). Final list is based on permit scope.
ETS-TE3	**Tool Isolation**	Each tool runs in a read-only container with user-specific working directories mounted at runtime. Containers cannot access the host OS or network.
ETS-TE4	**Execution Sandbox**	Applications are launched under sandboxing policies (e.g. AppArmor, SELinux) preventing calls to system-level resources or unauthorised filesystem access.
ETS-TE5	**Toolchain Immutability**	Users cannot install, update, or remove tools. Attempted package installations (e.g. pip, apt) are intercepted and blocked.
ETS-TE6	**User-Specific Workspaces**	Each user is granted a private execution environment (e.g. Jupyter kernel or R session) isolated from other users. Shared tools log all command history per user ID.
ETS-TE7	**Preloaded Libraries**	Tools include preloaded statistical, machine learning, and visualisation libraries (e.g. tidyverse, pandas, matplotlib) relevant to public health research.
ETS-TE8	**Blocked Features**	Tools with internet connectivity, plugin systems, clipboard exports, or external drives are stripped of those features or blocked at runtime.

6.7.4 Output Handling Infrastructure

This subsection defines how output files are managed within the ESPE environment, from creation by the data user to export review and authorised release by NeHA (Table **25**).

Table 25: NFR - ESPE - Output Handling

Code	Component	Specification

ETS-OH1	**Output Directory (User-Side)**	Each SPE includes a dedicated, permit-scoped ~/exports directory. Users move files they want to export here manually. This directory is monitored by the SPE operator.
ETS-OH2	**Export Submission Mechanism**	Once files are placed in ~/exports, users must tag them for review via an in-environment interface (e.g. button or command line). This initiates a request in the audit system.
ETS-OH3	**Export Queue**	Tagged files are moved to a secure Export Review Zone, accessible only by authorised NeHA SPE Operators. Users lose access to these files after submission.
ETS-OH4	**Operator Review Console**	Operators access a dedicated interface or secure shell to review export candidates. They may approve, reject, or request modification. Decisions are logged with justification.
ETS-OH5	**Export Policy Enforcement**	Exports are validated against permit terms and anonymisation standards. Outputs must contain only aggregated or de-identified content. Raw data is explicitly prohibited.
ETS-OH6	**Export Delivery Mechanism**	Upon approval, the system releases the file to the user via secure download (e.g. link in CY Login session) or encrypted email. Export logs track recipient, time, file hash.
ETS-OH7	**Rejected Outputs**	Rejected files are retained with the reason noted. The user may modify and resubmit, but cannot bypass the review step.

6.7.5 Audit Logging & Monitoring Stack

The ESPE must support full auditability and real-time monitoring across all user, operator, and system-level actions. Logging is essential for ensuring traceability, permit compliance, export control, and incident response under the EHDS regulation (Article 73) and GDPR accountability principles. All logs must be immutable, securely retained, and linked to the unique data permit identifier. Monitoring metrics must support proactive detection of performance issues or misuse (Table **26**).

Table 26: NFR - ESPE - Audit Logging and Monitoring Stack

Code	Component	Specification
ETS-AM1	**Action Event Logging**	All user and operator actions must be logged with timestamp, user ID, permit ID, action type, and system response.
ETS-AM2	**Event Coverage Scope**	Logs must include events such as login, logout, session timeout, file access, tool usage, export request, export decision, and system errors.

ETS-AM3	**Central Log Aggregation**	Logs must be sent to a central audit log service managed by NeHA. Logs are digitally signed and stored immutably.
ETS-AM4	**Log Retention Policy**	Logs must be retained for a minimum of 12 months after SPE VM decommissioning, per EHDS Article 73(1)(f).
ETS-AM5	**System Monitoring Metrics**	SPEs must emit system metrics (CPU, RAM, disk, session uptime) to the central observability platform in real time (minimum every 60 seconds).
ETS-AM6	**Alerting and Anomaly Detection**	Anomalies (e.g. high CPU, unauthorised tool execution, blocked export attempt) must trigger alerts visible to NeHA operators in their admin console.
ETS-AM7	**Error Traceability**	All user-visible errors, failed operations, and session terminations must be logged and classified in the log store for troubleshooting and compliance inspection.

6.7.6 Provisioning, Termination and Retention Rules

The ESPE must support a fully automated and controlled lifecycle tied to the data permit validity period. Provisioning, decommissioning, and data retention must adhere strictly to EHDS Article 68(12), which mandates that SPEs and associated data must be destroyed no later than six months after permit expiry. This section defines the technical rules and triggers governing these operations (Table **27**).

Table 27: NFR - ESPE - Provisioning, Termination and Retention rules

Code	Component	Specification
ETS-PT1	**Permit-Triggered Provisioning**	An ESPE VM must only be provisioned once the data permit is approved and the prepared dataset is available from the ISPE.
ETS-PT2	**VM Metadata and Tagging**	Each SPE VM must be tagged at creation with the permit ID, user ID(s), creation timestamp, expiration date, and tool profile.
ETS-PT3	**Access Enablement Notification**	Data users may only access the SPE after explicit provisioning completion and notification from NeHA via secure channel.
ETS-PT4	**Expiry and Auto-Deactivation**	At permit expiry, the SPE must auto-lock user access and suspend the VM. Users may no longer access the environment.
ETS-PT5	**Post-Expiry Retention Timer**	A retention timer (max 6 months) must be applied automatically upon permit expiry. After this period, full deletion is triggered.
ETS-PT6	**Destruction and Logging**	Upon expiry of the retention timer, the VM, volumes, datasets, and scratch space must be securely destroyed. A destruction log must be generated.

ETS-PT7	**Archival of Permissible Artifacts**	Optional approved scripts or final exported files (after approval) may be archived under NeHA internal archive policies if allowed by the permit.

7 SHARED SPECIFICATIONS (ISPE AND ESPE)

Both the Internal and ESPEs implemented under CY-EHDS-2nd are subject to a set of shared constraints that define a unified security, compliance, and operational baseline. These shared specifications are technical and procedural controls that apply identically across both SPE types, regardless of user role or data access modality.

This chapter 7 consolidates all such shared elements. Section 7.1 lists the NFRs that were excluded from Chapters 5 and 6 to avoid duplication. Section 7.2 documents the technical specifications implemented consistently across all SPE instances, including virtualisation, isolation, and logging standards.

7.1 Shared Non-Functional Requirements (SPE)

This section defines NFRs that are identically applicable to both Internal and ESPEs. These cross-cutting constraints ensure security, traceability, and operational consistency regardless of SPE type. They are enforced uniformly across the infrastructure managed by NeHA under CY-EHDS-2nd and reflect requirements set out in the EHDS regulation (Table **28**).

Table 28: Shared SPE NFRs

Code	**SharedSPE-NFR1**
Requirement	**Network Isolation**
Description	Both SPEs must operate under strict network isolation, with no outbound or inbound internet access. All communication is restricted to internal, trusted services managed by NeHA.
Measure/Compliance Indicator	- Verified by firewall rule audits, zero external DNS resolution, periodic penetration testing, and enforced interface whitelisting.
Code	**SharedSPE-NFR2**
Requirement	**Zero Trust Enforcement**
Description	Access control in both SPEs must follow zero trust principles: authentication is required at each session step, least privilege applies to both users and operators, and intra-component segmentation must be enforced.
Measure/Compliance Indicator	- Validated via RBAC audits, identity segmentation reports, and operator privilege logs.
Code	**SharedSPE-NFR3**
Requirement	**Immutable Audit Logs**
Description	Logs must be immutable, cryptographically signed, and centrally retained for at least 12 months after the decommissioning of the SPE instance.
Measure/Compliance Indicator	- Verified via log integrity checksums, WORM storage flags, and centralised retention logs.
Code	**SharedSPE-NFR4**
Requirement	**Toolset Immutability**
Description	Only the toolset explicitly approved during provisioning may be used. Users may not add, modify, or remove tools or libraries.

Measure/Compliance Indicator	- Measured via static container image validation, runtime enforcement of blocked install commands, and digital signature verification.
Code	**SharedSPE-NFR5**
Requirement	**Service Availability**
Description	The hosting platform must provide 99% uptime for both Internal and ESPE s during their active access windows, excluding scheduled maintenance.
Measure/Compliance Indicator	- Measured via observability metrics, uptime monitors, and automated incident resolution logs.
Code	**SharedSPE-NFR6**
Requirement	**Permit-Scoped Traceability**
Description	All operations—data access, processing, export, review—must be traceable to a unique data permit or data request ID, which must be applied across SPE components and logs.
Measure/Compliance Indicator	- Validated by tag propagation across logs, export metadata, dataset folder structures, and file lifecycle trackers.

7.2 Technical Specifications (SPE)

This section outlines the common technical specifications that are foundational to both the ISPE and ESPE within the CY-EHDS-2nd infrastructure. These shared specifications ensure a consistent technical baseline across all SPE instances, promoting security, interoperability, manageability, and compliance, in alignment with the CY-EHDS-2nd General Infrastructure and relevant EHDS regulation provisions.

The specifications listed herein represent overarching principles or common technical requirements that apply regardless of the specific SPE type (Internal or External). Detailed implementations or type-specific extensions of these principles are further elaborated in the dedicated technical specification sections for the ISPE (Section 5.5) and the ESPE (Section 6.7). This shared section serves as a common reference point, ensuring that both SPE types are built upon a unified and secure technical foundation (Table **29**).

Table 29: Shared SPE Technical Specifications

Code	Component	Specification
SharedSPE-TS1	OS Templates	All SPE VMs MUST be provisioned using standardized, security-hardened Operating System templates, managed and updated by NeHA.
SharedSPE-TS2	Tooling Containerization Principle	Where applicable and feasible for the specific SPE type and its tools, analytical tools and their dependencies SHOULD be deployed using container technology (e.g. Docker) to enhance consistency, isolation, and manageability. Container images MUST be from trusted sources and subject to security vetting.
SharedSPE-TS3	Controlled Data Exchange	All data exchange with SPEs (e.g., data ingestion, authenticated user sessions, results export) MUST occur via secure, controlled, and audited mechanisms defined by NeHA and aligned with the CPL. Specific interface details are defined per SPE type.
SharedSPE-TS4	Encrypted Internal System Communication	All necessary network communications between SPE components and other CY-EHDS-2nd central services (e.g. CPL for authentication/authorisation, shared observability stack for logs/metrics) MUST use mutually authenticated mTLS or equivalent secure protocols.

SharedSPE-TS5	Adherence to Centralized RBAC	SPEs MUST be designed to respect and enforce RBAC decisions managed by the CY-EHDS-2nd CPL. Access to SPE functionalities MUST align with roles assigned and verified by the CPL.
SharedSPE-TS6	Data Encryption at Rest Mandate	All persistent storage used by SPEs that may contain health data (raw, pseudonymized, or aggregated), intermediate processing files, or sensitive configurations MUST be encrypted at rest using NeHA-approved cryptographic standards (e.g. AES-256). Key management MUST be governed by NeHA policies.
SharedSPE-TS7	Client Endpoint Security Consideration	While NeHA secures the SPE infrastructure, users and operators accessing SPEs MUST be advised of their responsibility in securing their client devices. NeHA MAY issue security guidelines for client endpoints.
SharedSPE-TS8	Logical Data Scoping to Permits	All data processed or stored within any SPE instance MUST be logically scoped and strictly bound to the terms of the authorising data permit or data request ID. Technical measures MUST prevent unauthorised data co-mingling or cross-permit access.
SharedSPE-TS9	Goal of Automated Lifecycle Management	The provisioning, configuration, and decommissioning of SPE instances SHOULD be automated to the greatest extent technically feasible, driven by triggers from the DAAMs concerning permit issuance, modification, and expiry, and orchestrated via the CPL.
SharedSPE-TS10	SPE Log Integration with Central Stack	All SPE instances (Internal and External) MUST generate audit logs for SPE-specific activities. These logs MUST be securely transmitted to, or made accessible by, the CY-EHDS-2nd central observability stack, which is managed under the governance of the CPL (CPSS4). SPE-generated audit logs SHOULD incorporate common identifiers (e.g. Permit/Request ID, CPL-issued User/Session ID, Correlation ID where available from CPL) to facilitate end-to-end traceability and correlation with logs generated by the CPL and other CY-EHDS-2nd components.

8 ALIGNMENT WITH THE EHDS REGULATION

This chapter 8 details the alignment of the CY-EHDS-2nd SPE, as specified in this Deliverable (D7.1), with the legal requirements stipulated in EHDS regulation.

The establishment and operation of SPE for the secondary use of electronic health data are primarily governed by Article 73 of the EHDS Regulation. Given that the SPE is a critical national component for which the HealthData@EU CP R3 deliverables do not provide a ready-made, adoptable solution for Member States, it is imperative for the CY-EHDS-2nd project to meticulously design and specify its SPE in direct and demonstrable alignment with the Regulation. This chapter serves to provide that explicit demonstration, ensuring that the provisions for SPEs outlined in the EHDS Regulation are comprehensively addressed by the proposed Cypriot solution.

This chapter will therefore systematically address each relevant provision of Article 73, explaining how the design, technical specifications, and operational measures of the CY-EHDS-2nd SPE (encompassing its ISPE, ESPE, and shared components) ensure compliance. The CY-EHDS-2nd project is committed to upholding the high standards of data protection, security, and controlled access mandated by the EHDS Regulation. The alignment described herein is achieved through a combination of robust technical safeguards, clearly defined

organisational responsibilities (primarily vested in NeHA as the designated HDAB), and transparent operational procedures, all designed to protect the fundamental rights of natural persons while enabling the valuable secondary use of health data for purposes in the public interest. Reference is also made to Deliverable D0 'CY-EHDS-2nd CP for the overarching national architecture within which the SPE operates and for its integration with other national components and central services like the CY-EHDS-2nd CPL.

8.1 Overview

Article 73 of the EHDS Regulation sets forth stringent requirements for SPEs to ensure that the secondary use of electronic health data is conducted with a high level of security, data protection, and respect for the rights of natural persons. The CY-EHDS-2nd SPE, comprising both an ISPE for data preparation by NeHA operators and an ESPE for data analysis by authorised Health Data Users, has been designed to meet these obligations comprehensively.

Key principles of Article 73 addressed by the CY-EHDS-2nd SPE include:

- **Restricted and Authorised Access:** Ensuring only explicitly authorised natural persons listed in a data permit can access the SPE for defined purposes.
- **Prevention of Unauthorised Data Disclosure:** Implementing technical and organizational measures to prevent copying, downloading, or transfer of data or results that could lead to the re-identification of individuals.
- **High Levels of Data Protection:** Designing the SPE for robust confidentiality, integrity, and security of the processed data.
- **Comprehensive Audit Logging:** Maintaining identifiable and immutable logs of all access and processing activities within the SPE.
- **Implementation of State-of-the-Art Security Measures:** Committing to recognized security practices and ongoing review.
- **Data Minimisation by Design:** Ensuring only necessary data is processed for the specified purpose in the data permit.
- **Operational Integrity:** Including provisions for regular audits and adherence to implementing acts to be detailed by the EC.

The design of the CY-EHDS-2nd SPE, including its technical specifications, FRs, NFRs, and operational procedures described throughout this Deliverable (D7.1), collectively contributes to fulfilling these EHDS mandates.

9 CONCLUSIONS AND NEXT STEPS

In this deliverable we have laid the critical groundwork for establishing the national SPE of Cyprus. In this context we have defined the FRs, NFRs, and technical specifications for a robust, two-tier SPE model. This model comprises an ISPE, designed for secure data preparation by the HDAB (NeHA), and an ESPE, which will provide a controlled and isolated analysis environment for authorized Data Users.

Cyprus currently has no existing national SPE infrastructure dedicated to the secondary use of health data as envisioned by the EHDS. Therefore, D7.1 represents the foundational blueprint for a completely new,

essential capability within the Cypriot eHealth ecosystem. In developing these specifications, we have drawn inspiration and practical insights from established SPE implementations in other European Member States (such as Finland's Kapseli, France's HDH, and Belgium's Sciensano) and have been significantly aided by the knowledge sharing and collaborative environment of the EHDS2 Community of Practice, which has been invaluable in our journey to understand the multifaceted aspects and core concepts of SPEs.

Our primary design imperative has been to ensure that the national Cypriot SPE is fully aligned with the legal mandates and spirit of the EHDS Regulation (EU) 2025/327, particularly the stringent requirements of Article 73. Key elements of our SPE infrastructure, designed to achieve this alignment, include:

- **Strict, Permit-Based Access Control:** Leveraging the CY-EHDS-2nd CPL for strong authentication (CY Login & mTLS) and ensuring access is granted only to explicitly authorized individuals for defined purposes as per data permits managed via DAAMs.
- **Robust Data Security and Confidentiality:** Implementing measures such as encryption of data at rest and in transit, stringent network isolation with no direct internet access, and controlled data export mechanisms limited to non-personal, aggregated, or de-identified results following NeHA review.
- **Comprehensive Auditability and Traceability:** Ensuring all significant actions within the SPE are logged in an identifiable and immutable manner, integrated with the central CY-EHDS-2nd observability stack.
- **HDAB Governance and Operation:** Confirming NeHA role as the designated HDAB and sole operator, responsible for the governance, security, and operational integrity of the SPE.

In essence, D7.1 provides the essential architectural and operational specifications necessary to proceed with confidence towards building a compliant, secure, and effective SPE for Cyprus.

9.1 Next Steps

The completion of D7.1 marks a significant milestone, transitioning the SPE component from conceptualization and specification to the next critical phases of the CY-EHDS-2nd project. Key future plans and next steps include:

1. **Pilot Implementation and Testing:**

   The immediate next step involves moving towards the pilot implementation of the national Cypriot SPE. This pilot phase will be crucial for:

   - Developing and deploying the technical components of both the Internal and ESPEs based on the specifications outlined in this deliverable.
   - Testing the operational workflows, security controls, and user interfaces in real-world or simulated use case scenarios.
   - Validating the integration of the SPE with other CY-EHDS-2nd components, particularly the CPL for authentication and the processes for receiving permit information originating from DAAMs.
     This pilot will be conducted under the direct responsibility and oversight of NeHA, allowing for iterative refinement and practical learning.

2. **Alignment with Evolving EU Guidance and Specifications:**

The EHDS ecosystem is dynamic, and we are committed to ensuring the national Cypriot SPE remains fully aligned with EU-level developments. We are actively monitoring and anticipate incorporating:

- **Official Technical Specifications from TEHDAS2 for SPEs:** As these become available, they will inform the detailed technical build and operational procedures of our SPE.
- **EHDS Implementing Acts:** We await the Implementing Acts to be adopted by the EC by March 2027 (pursuant to EHDS Regulation Art. 73(5)), which will provide definitive technical, organizational, and security requirements for SPEs. The Cypriot SPE will be fully aligned with these acts.
- **Insights from the EU SPE developed under HealthData@EU:** We will also learn from and consider the architecture and operational model of the central SPE being developed as part of the HealthData@EU infrastructure, especially for ensuring interoperability in cross-border scenarios.

3. **Iterative Development and Operational Rollout:**

   Following a successful pilot, the SPE will move towards a phased operational rollout. This process will involve continuous improvement based on pilot feedback, evolving EU standards, and national priorities, with the ultimate goal of providing a robust and sustainable SPE service for the Cypriot health data ecosystem. Ongoing training for NeHA operators and awareness-raising for potential data users will also be key components.

10 REFERENCES

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

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

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

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

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

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

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

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

9. **TEHDAS2 (2025)**. *Draft Guideline on How to Use Data in a SPE (Milestone 7.1)*. TEHDAS2 Project, January 2025.

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

11. **Findata** (2025). *Kapseli®.* Helsinki: Findata, May 2025. URL: https://findata.fi/en/kapseli/

12. **Health Data Hub** (2024). *Health Data Hub – Overview.* Paris: Health Data Hub, February 2024. URL: https://catalogues.ema.europa.eu/institution/3331159

13. **Sciensano** (2023). *Healthdata.be.* Brussels: Sciensano, December 2023. URL: https://healthdata.sciensano.be/en