Ministry of Health, Welfare and Sport

health RI
enabling data driven health & life sciences

ICTU

National Institute for Public Health and the Environment
Ministry of Health, Welfare and Sport

Health Data Access Body-NL
Denk mee. Praat mee. Bouw mee.

Project acronym: HDAB-NL
Project title: *Establishing the coordinating Health Data Access Body in the Netherlands and its supporting digital business capabilities*
Number of grant agreement: 101128662
Call identifier/ ID of the action:
Topic: D8.1: X-BORDER GATEWAY and NATIONAL CONTACT POINT Requirements and Specifications – INFRASTRUCTURAL ARCHITECTURE
Starting date of the project: December 1st, 2023
Duration of the project: 4 years (December 1st, 2027)
Work package (task): WP8 (Infrastructural Solutions)
Submission date of deliverable: 01 May 2025
Dissemination level: PUB

Co-funded by the European Union

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 the European Health and Digital Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Document information (version 3.0)

Authors

Lead Author(s)	Lead organisation
Raymond ter Bogt	HDAB-NL WP8 lead, ICTU
Justin Poelstra	HDAB-NL WP8, ICTU
Daan Swinkels	HDAB-NL, CBS
Jeroen Beliën	HDAB-NL, Health-RI
Helen Hukshorn	HDAB-NL, ICTU Legal workgroup lead
Anne van der Kant	HDAB-NL, Health-RI
Thomas Hellebrand	Ministry VWS – reviewing and alignment WP10

Document history

Date	Version	Editor/Reviewer	Change	Status
07/02/2025	0.9	Raymond ter Bogt Justin Poelstra	1st Draft for Internal Milestone	Draft deliverable
10/02/2025 & 12/02/2025	0.9 and 0.99	Helen Hukshorn, ICTU	Internal legal review	2 reviews
07/02/2025	0.9	Daan Swinkels, CBS Thomas Hellebrand, VWS	Feedback of internal review processed	2 reviewers 2 reviews
12/02/2025	0.99	Raymond ter Bogt Justin Poelstra	Final Draft Internal Milestone D8.1 (4 reviews done)	Final reviewed Deliverable (technical)
07/02/2025-13/02/2025	0.99	Thomas Hellebrand, VWS	Feedback of two internal reviews processed	Final review on 13/02/2025
19/02/2025	1.0	TO	Review of version 1.0	No Go recommended improvements
03/03/2025	1.1	Daan Swinkels, CBS	Architecture and Requirements	Updated content on version 1.1
03/03/2025	1.1	Daan Swinkels, CBS	Business Capabilities & Component Model	New Content on version 1.1
03/03/2025	1.1	Helen Hukshorn, ICTU	Analysis of applicable EHDS Regulatory articles, considerations, and	New Content on version 1.1

			cross-reference to (in particular) other applicable EU (and NL) Regulations	
06/03/2025	1.2	Jeroen Beliën, Health RI	Technical Approach – Federated Architecture and Other approaches in the Netherlands	New Content on version 1.2
10/03/2025	1.2	Daan Swinkels, CBS	Descriptions of capabilities New appendix with full text description on Capability Model	New Content on version 1.2
14/03/2025	1.3	Cor Melse, RIVM	Generic Services	New Content on version 1.3
17/3/2025	1.3	Michiel Punt, SURF	Federated Global Research Network Standards & infra components; inventory IST	New Content on version 1.3
18/3/2025	1.3	Results of the Quarterly Session of the HDAB-NL incorporated into the Strategy discussion of HDAB-NL scope for WP8.1/2	Three scenarios that influence the scope discussion of the implementation of the D8.1 deliverables	New Content on version 1.3
19/3/2025	1.3	Writers' session WP8		
20/3/2025	1.3	Writers' session WP8 Technical Work sessions WP1 (Jochem)	Flows on the DAAMS and SPE processes	
24/3/2025	1.4	Writers' week HDAB-NL Strategic/Roadmap direction	Starting of the new WP8 coordinator with impact to the D8.1 deliverable	New Content on Version 1.4
25/3/2025	1.4	Writers' week HDAB-NL Scenario's and finalisation of Chapter headers		
26/3/2025	1.4	TO Meeting including New Feedback and Q&A	Final Documentation start	New Content on Version 1.4 4 sub-documents to reduce the final report
27/3/2025	1.4	Writers' week	Finalisation of Ch. 2-4	
28/3/2025	1.4	Writers' week	Alignment WP6	New Content Jeroen
31/3/2025	1.4	Delivery Week	Alignment WP5 Alignment WP7	New Content Anne

				New Content Daan
7/4/2025	1.5	Feedback week	Receipt of Feedback TO	Analysis & planning following feedback
8/4/2025	1.5	Meeting regarding transfer to Jasper van der Zwaag WP8	Meeting transfer documentation and Version 1.5 of delivery document	Proceed with action list (Checklist Changes April-2025)
10/4/2025	1.6	Processing 36 out of 39 action items & total replacement diagram Generic Functions	Finalisation document Monday 14/4/2025 (4 action items)	Evaluation final document with stakeholders
14/4/2025	1.6	Delivery Iteration 2	Finalisation & decision document voor TO	Approval request
18/04/2025	1.8	Delivery Iteration 3	Finalisation & decision document voor TO	Review CBS final comments
23/04/2025	1.8	Delivery Iteration 4	Finalisation & decision document voor TO	Review H-RI final comments
24/04/2025	1.9	Last comments processed	Finalisation & decision document voor TO	Final adjustments before submitting
01/05/2025	2.0	Final Document	Approval 30/04/2025	Approved and submitted to Steering Committee (SG).
30/09/2025	3.0	EU comments processed	Finalisation EU comments	For review

1 Executive Summary

Deliverable 8.1 has been given the scope to rigorously explore and map the requirements and specifications of the HDAB infrastructure.

This is roughly divided into two parts:
1. The picture at the EU – with two 'corners' in the overall four-corner architectural model
2. The picture in the Netherlands – with two of those four 'corners' in this model

The components of the infrastructure on the EU side are determined by Central Services. The components on the Dutch side are closely related to the technical work package requirements. These are related to EHDS requirements and specifications for all technical packages in general and some packages in particular, plus, where available in the future, the implementing act(s). Because these are not yet available, this document becomes an incremental state-of-the-architecture 2025 and cannot therefore be treated as a potential view of any end-state architecture.

The deliverables of WP8 from the Grant Agreement are introduced in chapter 3. The definition and description of the technical capability building blocks is further elaborated in chapter 4. Then, in chapter 5, the alignment with a potential process architecture is done. In this chapter the technical work packages requirements are linked together into a potential technical architecture of the National Contact Point for secondary use. Based on the described building blocks the current Dutch situation is then explored.

Finally in chapter 6, the EHDS text is comprehensively explored, and all relevant articles are identified and explained in detail. This document is wrapped up by briefly touching upon a taxonomy for the collection and organisation of architectural requirements in chapter 7. This document concludes with a glossary in the Appendix, in which the technical terms are explained.

Table of Contents

2 Preface

2.1 Incremental state of architecture

EHDS Article 75, paragraph 12 states that "by two years from the date of entry into force of this Regulation [by 2027], the Commission shall, by means of implementing acts, set out:

- Requirements, technical specifications, and IT architecture of HealthData@EU
- Conditions and compliance checks required to be able to join and remain connected to HealthData@EU
- Minimum criteria that need to be met by the national contact points for secondary use and the authorised participants in HealthData@EU

The current state of architectural choices and options contains many uncertainties and a high level of subjectivity of options available. This means that all requirements and specifications in this document are subject to change until implementing acts are in place. No rights and/or obligations can be enforced by implementing parties until such time, but in the meantime the HDAB-NL program, work package 8, attempts to design and develop the minimal viable infrastructural product, required of this IT architectural design for secondary utilisation of healthcare data on the Dutch side.

The minimal viable product is achieved through a short series of a PoC and Pilot, followed by an agreed upon implementation that will be handed over to the future Health Data Access Body, that in-turn will further implement and develop it into its end-state requirements and specifications. The architectural design, therefore, is meant to be incremental and thus, this document is a living document that will be further updated in the future. The current state of the architectural discovery and design has been based on the ideas of the program, its internal and external participants, and the participants of related programs within the Netherlands and in the EU.

2.2 Abbreviations

This document contains many abbreviations and jargon. The most prevalent terms can be found in the following sections.

Abbreviation	Description
API	Application programming interface
CBS	Centraal Bureau voor de Statistiek, Statistics Netherlands
DAAMS	Data Access Application Management solution
DPO	Data Protection Officer
EDPB	European Data Protection Board
EEA	European Economic Area
EHDS	European Health Data Space
EA	Enterprise Architecture
EU	European Union
GDPR	General Data Protection Regulation
HDAB	Health Data Access Body (the *organisation*)
HDAB-NL	Health Data Access Body in the Netherlands (the *programme*)
HDC	HDAB Health Data Catalogue
HealthData@EU	Cross-border infrastructure as defined in Art. 75 EHDS Regulation
Health-RI	Foundation for Dutch health data research infrastructure
HLD	High Level Design
ICTU	Foundation for improvement of digitisation of Dutch government
LLD	Low Level Design
MVP	Minimal Viable Product
PoC	Proof of Concept
REST	Representational State Transfer, a software architectural style
RIVM	Rijksinstituut voor Volksgezondheid & Milieu, National Institute for Public Health and the Environment
PET	Privacy Enhancing Techniques
R&S or RS	Requirements & Specifications
SPE	Secure Processing Environment
SURF	IT service provider for Dutch education and research institutes
TEHDAS(2)	(Second) Joint Action Towards the European Health Data Space
VWS	Ministerie van Volksgezondheid, Welzijn en Sport, Dutch department of Health, Welfare and Sports
WP	Work Package within the HDAB-NL project

2.3 Terminology

The EHDS has defined important terminology in the context of DP8.1, which is relevant to this deliverable. The following definitions are introduced here to scope the analysis of requirements and specifications.

National Contact Point:
Organisation and technical Gateway for secondary use, enabling and responsible for the making available of electronic health data for secondary use in a cross-border context.

National Connector (now Dispatcher):
Software and infrastructural solution that is placed as an abstraction layer on the infrastructure architecture on the "National side." Its main function is to ensure that the interoperability from "NL to EU Central Services" and from "EU Central Services to NL" is established.

Cross-border gateway:
Software and infrastructural (portal) solution that is placed as a transmission and reception communications Node on the infrastructure architecture on the "National side." Its main function is to ensure that communication is secure and technical interoperability is standardised.

Cross-border engine:
Functional and software component developed (message) agent interfaces that are developed as an extension to HDAB functionality to manage the HDAB-micro service-architecture in an automated way.

Generic services:
There are at least three fundamental Generic Services required, as described in the EHDS:

1. Identification, a (legal) person must identify himself
2. Authentication, a (legal) person must prove his identity
3. Authorisation, a (legal) person derives specific access/permissions from his permit

Further generic services have been identified, but due to their provisional nature they will be addressed in the next phase of the programme.

3 Introduction to work package 8

3.1 Objectives of this work package as described in the Grant Agreement

The HDAB-NL project aims to establish the coordinating Health Data Access Body in the Netherlands together with its supporting digital business capabilities over a four-year period. Under the responsibility of the Ministry of Health Welfare and Sport (VWS) as beneficiary of the grant, the project will be conducted by a consortium consisting of ICTU (coordinator), Statistics Netherlands (CBS), Health-RI (HRI) and National Institute for Public Health and the Environment (RIVM). The work is divided into ten work packages, each led by one of the project consortium partners. Next to the four mandatory horizontal work packages (coordination, dissemination, evaluation, and sustainability) the project also includes six vertical, technical work packages – each aimed at developing the digital business capabilities under which a health data access body could operate successfully: data access application management system, health dataset catalogue, secure processing environment, cross-border gateway & generic services, data quality, and establishment of the coordinating health data access body.

The scope for WP8 in the Grant Agreement encompasses:

Cross-border gateway[1]:

- Connect to HealthData@EU infrastructure to enable cross-border workflows for secondary use of electronic health data at EU scale.
- Scrutinise existing requirements and specifications for the cross-border gateway for secondary use of electronic health data.
- Analyse the requirements and design the national connector responsible for connecting the cross-border gateway to the national infrastructure.
- Implement and pilot the cross-border gateway for secondary use of electronic health data.
- Launch an operational cross-border gateway for secondary use of electronic health data.

National contact point:

- In parallel of the technical work this connection requires, a decision-making process needs to be initiated, leading up to the appointments of where to host the connection with the HealthData@EU infrastructure (National Contact Point for the secondary use of health data).

Generic Services:

- Develop and deploy generic services that must be used in the work processes of the HDAB-NL, such as identification, authentication, authorisation, and localisation.
- Take inventory of the different generic services that are needed in the health data access body capabilities, as indicated by TEHDAS(2) work packages.
- Scrutinise existing requirements and specifications for the generic services.

[1] In the programme plan called the cross-border portal

- Tailor (in case of EU available) or develop, implement, and pilot the generic services in the cross-border gateway for secondary use of electronic health data.
- Successfully deploy generic services in the cross-border gateway for secondary use of electronic health data.

3.2 Milestones and deliverables

Work package WP8 has three deliverables (outputs/outcomes):

- D8.1. National connector for Cross-border gateway + Generic Services: checking and analysis of **draft requirements and specifications**.
- D8.2. Cross-border gateway + Generic Services: **Pilot a Minimal Viable Product (MVP)**, planned for by the end of 2026.
- D8.3 Cross-border gateway + Generic Services: **Operational Service (Operational Product)** to hand over by the end of Phase III (end of 2027).

The scope of the first phase (report) is deliverable D8.1.

3.3 Legal context of WP8

3.3.1 Current legal context as the basis for analysis

The final[2] EHDS-text is the primary resource for the scope of the Minimal Viable Product. A joint analysis was performed by all technical work package architects to inventory all relevant requirements and specifications-sets. In this report we focus on the sections regarding:

- Secondary use of electronic health data.
- National contact point and cross-border infrastructures for secondary use.
- Generic services.

The full EHDS text-analysis and results can be found in chapter 6. Secondary relevant regulations that, without prejudice, are as equally important as EHDS to the requirements and specifications are listed in this document as well. The MVP to be piloted in the next phase will be limited to the **legally required scope** of the Design specification (only the MUST HAVES[3] apply).

3.3.2 Iterative work in progress

As mentioned, this document is a living document. Current and future Geopolitical changes impact the choice (within the EU) of the Solution and Software architectural directions. National and international infrastructural adjustments are yet unclear and uncertain at the close of D8.1. Changes in the deployment and utilisation of critical infrastructures may occur.

Updated versions are to be expected throughout the project when:

[2] March 5, 2025: https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_en

[3] Partly based on recommendations of the Legal workgroup that was led by the ministry of VWS.

- National implementing legislation is put into place related to the implementation regulations of the EHDS and the specific changes around the Government digitalisation initiatives.
- New insights arise within the Joint Action Towards a European Health Data Space. Recommendations for implementation acts, will be incorporated, which also creates the need to harmonise HDAB-NL infrastructure specifications with TEHDAS(2).
- After evaluation of lessons learned from the HealthData@EU pilots, including the to be planned Hackathons, starting Q2-2025.
- After evaluation of lessons learned from/during the pilot phase in NL.

Due to these constantly changing parameters, work package 8 delivery will remain an iterative work-in-progress.

3.4 Architecture & structure for the programme

Within the context of HDAB-NL, this work package is also responsible for providing structure and overall architecture frameworks[4] for the technical work packages of the entire programme. This means that WP8 provides cross-work package inspiration on:

- Common architectural terminology in the vertical work packages.
- Common architectural framework in all work packages (including one program wide enterprise architectural framework: EAF[5]/NORA).
- Common technical vocabulary of logical architectural elements that will collaborate in the future platform of HDAB.

[4] The common (shared) architecture is analysed in chapter 7.

[5] The scope of WP8 is focused on the translation of EHDS into technical architectural building blocks, which form the TA layer of the EAF model. WP5, 6 and 7 have the BA layer as a starting point in Phase 1.

4 Description of first deliverable

T8.1 Cross-border gateway + generic services – analysis and design

The European Health Data Space Regulation aims to establish a secure and structured framework for sharing health data across Europe. EHDS, chapter IV of the regulation specifically addresses the reuse or *secondary* use of electronic health data, enabling access for research, innovation, policy-making, and other public health purposes. By fostering interoperability, privacy, and standardisation, EHDS seeks to unlock health data's potential for advancing healthcare and public health while maintaining rigorous data protection and security standards.
The HealthData@EU IT infrastructure aims to facilitate secure, interoperable information exchange between National Contact Points (NCPs) through a unified network, supporting various use cases as outlined by the EHDS. On the National side the unified EU network connects to one NL-National Connector, which in turn connects to the contributing Dutch participants. The technical specifications and open source codes for the implementation of the cross-border gateway and the connection to the central platform of the HealthData@EU are provided and published now under the Release 4 of the central platform documentation provided by the Commission.

The first step for a successful implementation of the Cross-border gateway solution is to start "Analysis and design" activities. In particular, the analysis of requirements and specifications and design of the national connector connecting the cross-border gateway to the national infrastructure, the analyses of the overall architecture in general and the generic services in particular[6].
Requirements and specifications are set in phase-II to be demonstrated with the use of a prototype supporting stakeholders to accurately understand the potential future HDAB National Connector and Generic Services.
These activities build upon the outputs from TEHDAS(2) and upcoming Joint Actions on secondary uses, as well as on the lessons learnt on the HealthData@EU Pilot, to ensure alignment and interoperability with the other HDAB's HDC. The design also includes an alignment with strategic choices and generic services for primary use of health data in the Netherlands, to ensure optimal synergy between primary and secondary use.

4.1 Overview of HealthData@EU target architecture

HealthData@EU has done preliminary development work on the infrastructural components and supported processes. TEHDAS 2 also has delivered initial insight into the functional and non-functional requirements of the future HDAB-architecture. The four-corner model, which is the fundament to the future solution architecture, is depicted here.
The following diagrams and descriptions are based on the EHDS Architecture Definition Document D5.1 (21NOV2024) of the HealthData@EU pilot.

[6] see SG231213-1 - Definitieve Grant Agreement HDAB-NL.pdf, section Infrastructural solutions (cross-border gateway + generic services)

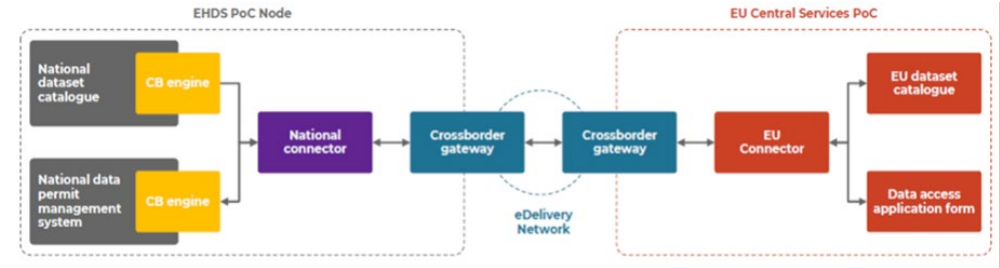


Diagram: four-corner model

The four corners are:

1. National Connector on NL-side
2. The Cross-border Gateway on NL-Side
3. The Cross-border Gateway infrastructure on HealthData@EU side
4. EU-connector for EU Central Services platform

These four corner were the starting point for the journey of Discovery for the Infrastructure Architecture building blocks on NL-Side.

In Malta, in March-2025 this had evolved into a discussion (all-2024) about the precise scope of the future solutions architecture. Although the platform design was still visible in its iconic four-corner model, the terminology of the entire infrastructure architecture had evolved into the following overall view:

1. HDAB Coordinator Portal on NL-side
2. National Contact Point, including the Member state Node that functions as the entry point into the NL-Side cross-border infrastructure
3. EU Central Platform (Cross-Border infrastructure)

4a. Union Contact Point, with its Union Service Portal

4b. Other Participant's Contact Point, for authorised access from third countries and international organisations

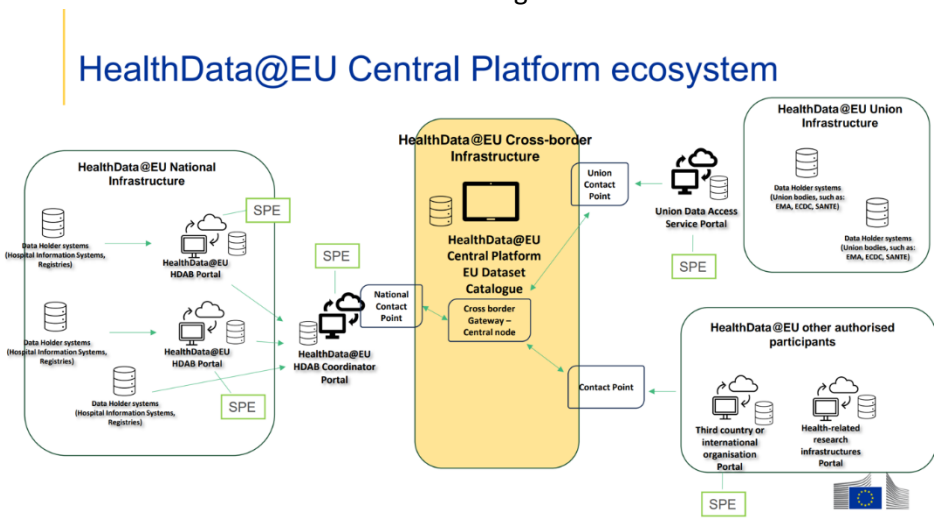


Diagram: Malta - General Assembly 2025 presentation of the Cross-Border infrastructure

The current state of the four-corner model has not only evolved in 2024, it also has changed in terms of clarity around the functional and non-functional requirements. This document reflects the state of insight of March-2025 and may therefore evolve as well.

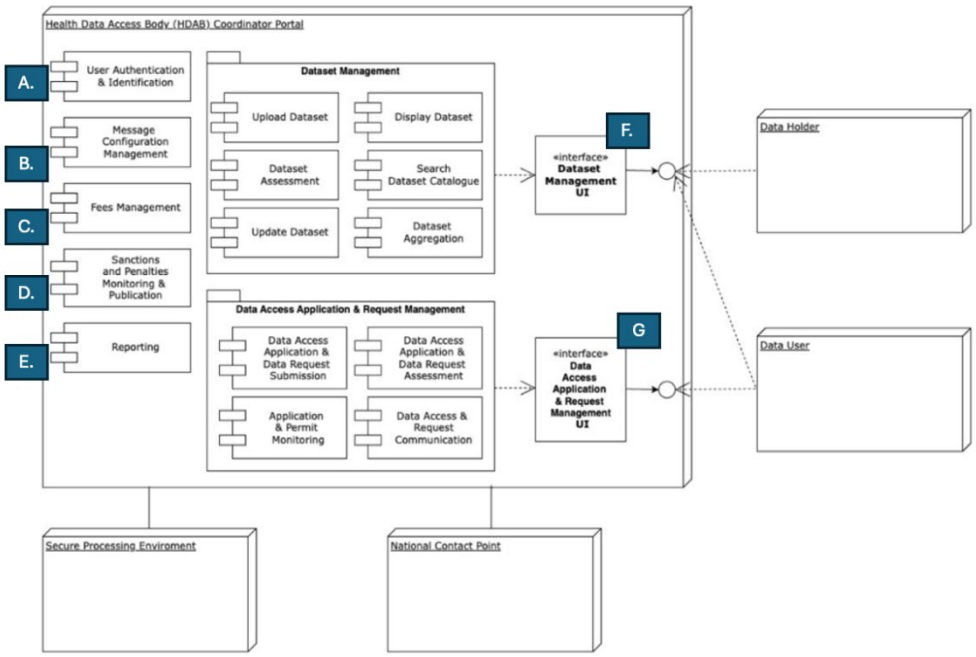
4.2 Building blocks

Deliverable D8.1 focuses on discovery and elaboration (conceptual and logical building blocks). In the next phase Physical Architectural Building blocks will be defined.

In the HDAB-NL programme, the infrastructural building blocks are treated as component (micro-)services or products, inside a larger framework of components that encompasses the entire HDAB-NL enterprise landscape.
In phase 2, the entire landscape, including required scenarios for physical INFRA, are presented as part of D8.2. Therefore, this is out of scope of D8.1.

4.2.1 Corner 1 - HDAB Coordinator Portal

The HDAB Coordinator Portal (in case of the Netherlands this is the “central” Portal in a potentially federated data landscape) is part of the HDAB organisation and contains the following functions:



Diagram; HealthData@EU HDAB Coordinator Portal architecture

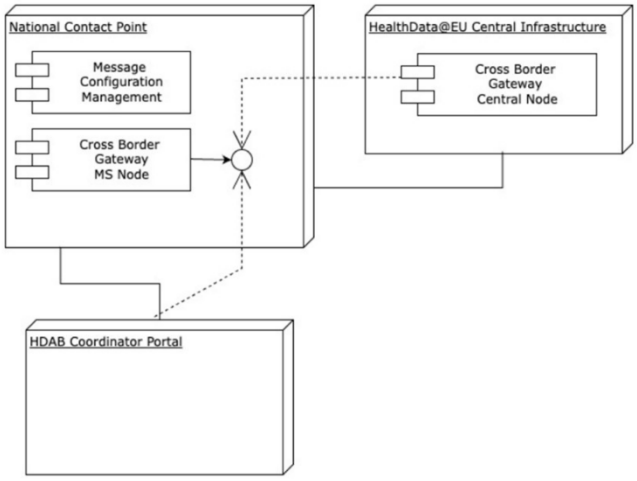
- A. User authentication, identification, and authorisation[7]: Validates an HDAB's, Data Holder's, or Data User's identity. In the case of a Data Holder, or a Data User, authentication validates a natural or legal person's identity desiring to either provide a dataset description or search for a dataset description, respectively. In the case of an HDAB, authentication verifies the identity of the user desiring to assess dataset descriptions and labels. Authorisation ensures the HDAB user in question has access to the system or resource with the required role(s).
- B. Message sender/recipient configuration management: Configures and formalises all business and technical rules to ensure efficient coordination between HDAB Portals and National Contact Points.
- C. Fees management interface to the NL-HDAB Business Finances Function: Calculated Fees will be transparently, non-discriminatory, and proportionately communicated to data users. These fees will be communicated before the submission of the data access application or request. Invoices to be paid will be sent directly or through the Cross-Border Gateway when the data permit is generated.
- D. Publication of sanctions and penalties at the national and EU level: Compliance monitoring with EHDS Regulation by data users and health data holders will be published. Corresponding sanctions at the national level will be determined and also sent through the messaging infrastructure. Local infringements are managed by the national infrastructure and are made available to the HealthData@EU Central Platform for republication at the EU level. This traffic is sent through the Member State Node.
- E. HealthData@EU Reports: HDAB generates a biennial activity report at the national level to be made publicly available on the HDAB website and disseminated to the EU Central Platform to be submitted to the proper EU-Supervisory Authorities. Reports can be either Management Reports (On performance and delivery of services) or Compliance reports (on compliance to Governance, Risk and Legal requirements to the HDAB).
- F. HDAB interoperability requires an integrated approach of SPE(s) and the Data Catalogue(s). The form of the integration depends on the infrastructural choices as well as the future Dutch Data Landscape. Business and Solutions Architectural choices to integrate this, will be made as of phase II.
- G. HDAB interoperability requires an integrated approach of Data Access Application and Request Management capabilities such as the DAAMS Solution(s). The form of the integration depends on the Solutions architectural choices as well as the future Dutch Data Landscape. Business and Integration Technology choices to integrate this, will be made as of phase II.

[7] CoP SG4 - SC022_D03.03_Architecture_Scale-Up_SANTE APPROVED

4.2.2 Corner 2 - National Contact Point (including Cross-Border Gateway)

The National Contact Point can be defined by the EHDS as an organisational entity as well as a technical platform, containing two functions. The two functions defined in the target architecture at HealthData@EU are:

1. It is a Message agent including configuration functionality.
2. It is a Member State Node that (**EHDS art. 75: Par 7**) "supports and facilitates[8] the cross-border access" to the HealthData@EU Central Node and, vice versa, the cross-border access to the Dutch network of (one or more) HDAB(s) and (one or more) SPE(s) - depending on the scenario that will develop in the future situation beyond 2027.



Diagram; National Contact Point (NCP)

The National Connector/Dispatcher is a software component exposing capabilities that are common to all National Contact Points to fulfil the user journey steps, such as connecting to and accessing and messaging at a DAAMS technology and SPE technology, but also to Catalogue platforms and/or solution architectures. EHDS (art.75, par.1) states that "each Member State shall designate one contact point for secondary use".

The main task of the National Connector is to add an abstraction layer before the Cross Border Gateway and therefore to expose specific features needed to fulfil the infrastructural use cases. An example of a use case for the National Connector is to ensure that an acceptance message of a 'data permit request' by the National Contact Point is correctly received and understood by the Central Services platform at HealthData@EU.

[8] The Node in this Figure is a (inter)connectivity medium between NL and EU for relaying contents regardless of content. It can be seen as the transport medium, which must support the required kinds of payload it transports. Specifications of this medium are therefore specific to the transport requirements and not to the kind of payload transported.

4.2.3 Cross-Border Gateway – Member State (MS) node

A Cross Border Gateway manages the transmission and reception of communications between National Contact Points and the Central Services in a secure and technically standardised manner. At the finalisation of this document, it is yet unknown what the technical architectural building blocks for the MVP will be. The core functional requirement for the memberstate node is to be:

- Security requirements have to be sufficient for the HDAB-required level.
- Standardised towards the EU-Central Services gateway.
- Standardised, Interoperable, and secure towards the NL-Coordinator Portal.

EHDS (art.75) states that there is one Cross Border Gateway instance for each National Contact Point. An example of a use case for the Cross Border Gateway is to send an acceptance message of a 'data permit request' from the National Contact Points' Cross Border Gateway to the Central Services' Cross Border Gateway.

4.2.4 Cross-Border Engine (Messaging API to Corner 1)

Cross Border Engines are extensions of the Health Data Access Bodies' (HDAB's) information systems (e.g. dataset Catalogues or data Permit Management Systems) that add new functionalities to the systems in order to enable cross border use cases. There can be one or more Cross Border Engine instance(s) for each application of an HDAB, e.g. one Cross Border Engine instance for the National Dataset Catalogue.

4.2.5 Infrastructural Generic Services

In this paragraph an attempt is made to interpret an early version of the NCP for secondary use as a conceptual portal architecture, based on existing Generic Services in NL:

- Three known Generic Services in relation to the processes described previously.
- Identifying what is known at this stage of Localisation.
- Identifying what is known at this stage of Addressing.
- Identifying what is known at this stage of an Opt-Out mechanism.

4.2.5.1 Generic Services: current understanding

Only three generic services are currently required. In chapter 6 further elaboration can be found on the following three:

- Identification.
- Authentication.
- Authorisation.

They are required when and if automatic forwarding is required from the HDAB Coordinator Portal to and from the DAAMS and the SPE. There are many uncertainties and unclarities as to the legal duty to deploy a Coordinator Portal within the Dutch participant network. At this stage it remains an open

question whether law dictates this. The legal workgroup will have to investigate this in more detail as the TEHDAS2-programme continues working on Implementing Acts.

Drawing up a potential infrastructural design is uncertain and still very complex due to the many potential implicit and explicit choices that must still be made at this stage. The diagram in this paragraph is for comparison and discussion purposes only and to contrast with the similar diagram drawn up for primary use[9].

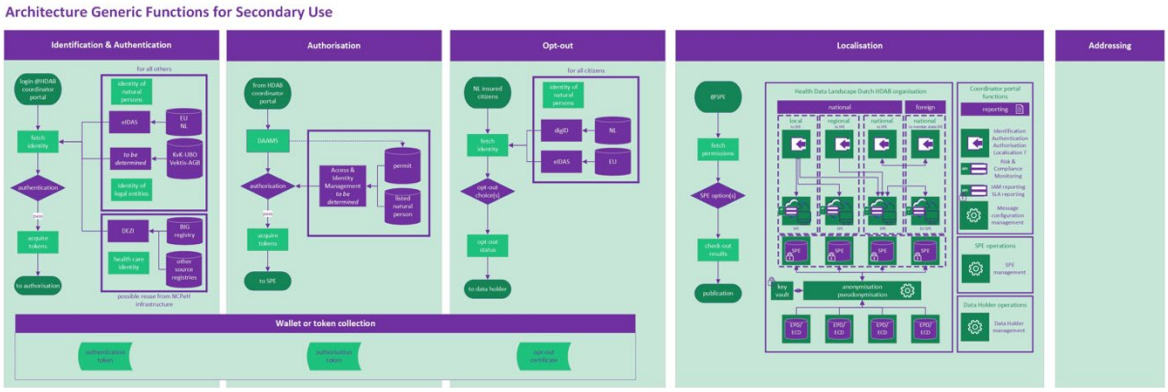


Diagram: Reasonably clear elements of Architecture of the NL-Generic Functions for Secondary Use – April 2025

At the point of finalising D8.1 there are no known Requirements and Specifications that have been finalised on the following subjects yet. They have been included for completeness's sake but have to be treated as provisional.

4.2.5.2 Localisation

Additionally, under the HDAB-NL programme, a fourth generic service is mentioned: Localisation. In primary use it applies to the location where data is stored. This does NOT apply in the same way for Secondary use, as more location data is required about both the Data Holder as well as the SPE.

From Localisation and other NEN[10]-norms we distinguish at least the following differences:

Localisation (or where health data is stored) can apply to different subjects and architecture layers:

- Localisation of (meta)data -> Relevant in the context of Findability of the metadata catalogue.
- Localisation of specific data records/information within datasets -> Also relevant to the catalogue on both (current) Local, Regional and National Level, as well as for the synchronisation between the National Catalogue and the EU-Catalogue.
- Localisation of permit grant/requestor -> This is relevant to the Application process rules set down in the EHDS, especially in relation to the infrastructure used (for example Cloud Computing or PaaS Solutions abroad.

[9] Comparison against https://www.datavoorgezondheid.nl/publicaties/publicaties/2025/03/13/architectuur-generieke-functies-2025

[10] See: https://www.nen-egiz.nl/start-van-de-publieke-commentaarronde-voor-de-norm-nen-7519-lokalisatie/

- Localisation of infrastructural services -> This is directly relevant to the Node and Messaging Agent under study. Localisation can refer to both the logical location of information (So within legal and practical control & Maintenance), as well as to the physical location (physical (IP-) addressing of the data, metadata, and reporting data).

All these differences are even more legally and operationally complex when applied in a Cloud computing context.

4.2.5.3 Addressing

Addressing is even more unclear and uncertain as a generic function. Therefore, it is purposefully left blank in comparison with the Architecture for generic services for primary use.

4.2.5.4 Opt-out mechanism

EHDS requires the possibility for a citizen to opt-out. No actual design and/or process is known yet at the finalisation of this document. The mechanism for primary use is an opt-in. This is NOT comparable to an opt-out process.

4.3 Joint logical process description of use cases of an MVP

In D8.1 the choices on scope of the pilot are not yet available. As a consequence, this document becomes an incremental state-of-the-architecture 2025 and cannot therefore be treated as a potential view of any end-state architecture for the HDAB future. In the following paragraphs the requirements for WP8 are analysed based on the process flows and events analysed in the current situation within the programme. In phase 2 the analysis will be further elaborated into Use Cases within the programme, depending on the insights that are currently work-in-progress.

In order of appearance the following design and analysis diagrams and to be elaborated functionalities and accompanying solutions have been documented for the scope of phase 1:

1. Catalogue functionality > Data Discovery: 7 steps on process level plus 7 sub-steps at INFRA level.
2. Catalogue functionality > Data request process > HDAB: 21 steps on process and solution level.
3. DAAMS > Data Permit application and
4. DAAMS > Updating the Permit application – at this level of sub-steps the outlines of potential piloting use cases become visible.
5. SPE > Data Use or Utilisation of data . The specific situation discovered is just one example of (potentially) many ways SPE(s) can be utilised within NL. It is up to the programme and its stakeholders in NL to determine which future variation may be further elaborated and developed beyond the initial tests and pilots. At the close of D8.1 these choices have not yet been presented or made.

The five logical designs (for discussion in phase I and elaboration for phase II) are documented in more detail in the following sub-paragraphs.

4.3.1 Catalogue functionality

In the inventory of an MVP there are at least two functionalities required to realize an MVP on the HDAB-NL program:
1. The HDAB shall implement a Data Discovery process and functionality including baseline infrastructure.
2. The HDAB shall implement a Data request process and functionality including baseline functionality of a DAAMS, an SPE and baseline infrastructure.

In the following paragraphs each are inventoried and explained integrally including the choices made by the technical work packages and their impact on the D8.1 Deliverables required.

4.3.1.1 Data discovery process (logical)

Data discovery : publish/update the EU Dataset Catalogue (**ACCESS** and **UPDATE**-services)

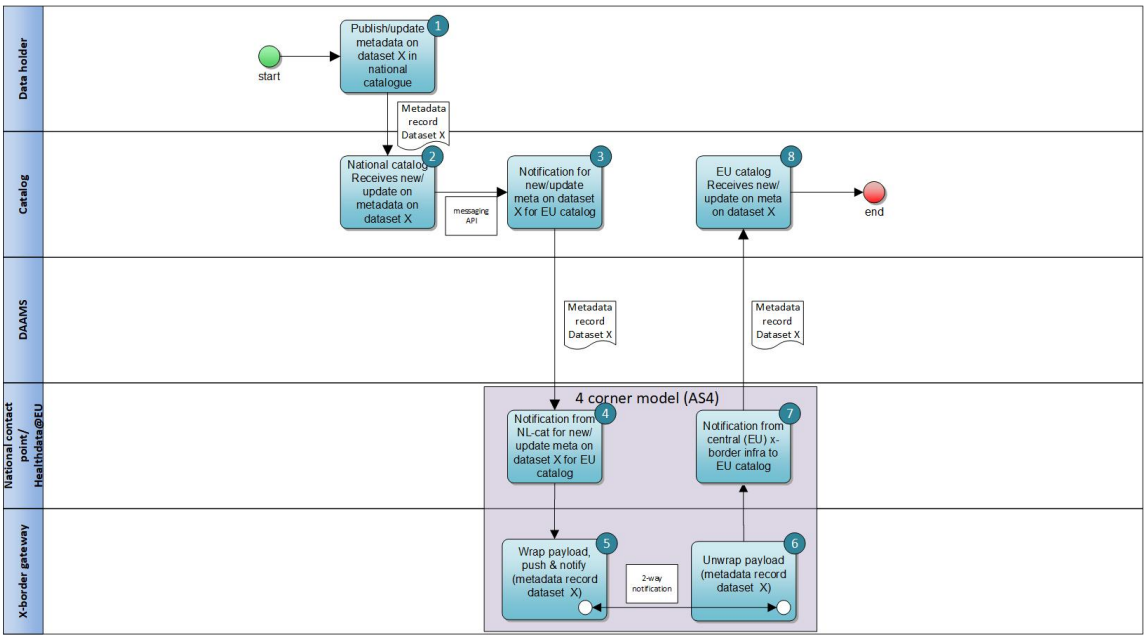


Diagram: Provisional overall workflow to publish/update metadata in the EU Dataset Catalogue

1. The data holder has a NEW or UPDATED metadata record about dataset X and wants to publish that to the national catalogue as well as the EU central service catalogue. The metadata record will be made available via a FAIR Data Point (FDP) or by manual entry within the national catalogue itself (then step 2 will be skipped).

2. The national catalogue will check the known FDP at regular intervals for NEW or UPDATE metadata records of datasets and once found and checked on validity harvest them (make them available) inside the national catalogue.

3. The national catalogue will make the NEW or UPDATE records known so that external systems like the Cross Border Engine can manage the change towards the EU central catalogue

4. The Cross Border Engine is in charge of identifying when there is a change on the national dataset catalogue. The National Connector sends the NEWLY VERSIONED description of the dataset in HealthDCAT-AP to the National Cross-Border Gateway.

5. The National Cross-Border Gateway sends an eDelivery message including the metadata record of dataset X over the network to the EU central platform Cross Border Gateway, leveraging all security features of eDelivery (encryption, authentication).

6. The EU central platform Cross-Border Gateway manages the received eDelivery message and makes it available for processing by the EU connector.

7. The EU connector reads all eDelivery messages. Once a new data discovery message is received, it performs the associated action on the EU Dataset catalogue (create, update, delete, restore) (8) and the NEW or UPDATED metadata record of dataset X is available in the EU central catalogue.

The technical (WP8) flow and description of the Cross-Border gateway is depicted in the Diagram below.

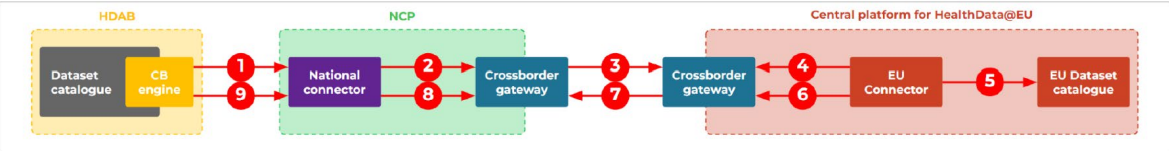


Diagram: Workflow to update the EU Dataset Catalogue

1. The Cross-Border Engine is in charge of identifying when there is a change on the national dataset catalogue. It then calls the APIs of the National Connector with the NEWLY VERSIONED description of the dataset in DCAT-AP.

2. For data discovery, the National Connector exposes four REST-APIs (create, update, delete, restore). When one of those APIs is called, the National Connector prepares the eDelivery message (encoding to base 64, authentication to eDelivery) and sends it to the National Cross-Border Gateway.

3. The eDelivery message is sent over the network to the central platform Cross-Border Gateway, leveraging all security features of eDelivery (encryption, authentication).

4. The EU connector reads all eDelivery messages.

5. Once a new data discovery message is received, it performs the associated action on the EU Dataset catalogue (create, update, delete, restore).

6. Depending on the success of the operation, the EU connector prepares the eDelivery message (encoding to base 64, authentication to eDelivery) containing the status of the operation and sends it to the central platform Cross Border Gateway.

7. The eDelivery message is sent over the network from the EU Central platform (back) to the national Cross-Border Gateway, leveraging all security features of eDelivery (encryption, authentication).

8. That status of the operation is stored in the database of the National Connector.

9. The Cross-Border Engine can check the status by calling an API endpoint of the National Connector. If it fails it can raise an alert to the end user managing the National Dataset Catalogue.

4.3.1.2 Data request; process (logical)

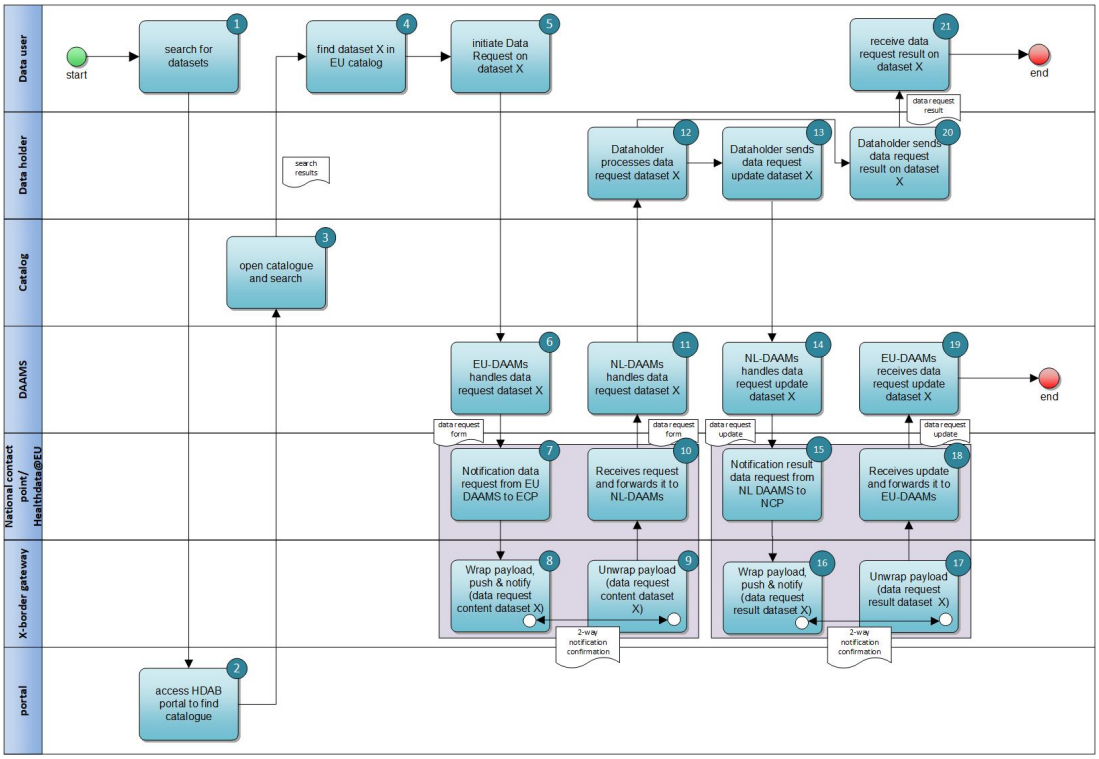


Diagram: Provisional overall workflow to find and execute a data request on dataset X

In this section data request and data access application are not separated yet, this distinction and implications for process flows will follow in next milestones and deliverables. Furthermore, though data requests and data access applications are different concepts from the DAAMS perspective, from the cross border infrastructure perspective the mechanisms are very similar and changes in payload of the messages/update/forms sent and received do no not require separate configurations.

1. The happy flow starts with a data user that wants to identify a dataset of interest.

2. The data user identifies via a portal the EU (central) catalogue to start looking for datasets of interest.

3. The data user opens the EU catalogue of interest and starts searching for a dataset.

4. Data user finds dataset X in the EU catalogue and wants to know the gender distribution on this dataset X (i.e. a data request)

5. Data user initiates a data request application on dataset X within EU catalogue.

6. Within the EU (central) DAAMS the data user completes the data request, and the EU DAAMS starts managing the data request in dataset X. The dataset X is from NL and EU DAAMS initiates process and forwards the data request to the NL-DAAMS.

7. The EU Contact Point (ECP) receives a notification of the forward (including data request) and applies the 4-corner principle and via 8 and 9 to the NL Contact Point 10 receives the forwarded data request and delivers it to the NL-DAAMS.

11. NL-DAAMS performs the internal DAAMS procedures and once all okay notifies the data holder of dataset X to execute the data request on dataset X 12 and return the result 13 to the NL DAAMS as well as to the data user 20.

14. NL DAAMS notifies the NCP (or the NCP notes there is a result) and the NCP 15 via the 4-corner principle sends the result via 16 and 17 to the ECP 18 The ECP sends the result of the data request to the EU DAAMS 19 which stores the results and closes the original data request application.

21 The data user receives the result (answer) on the data request on dataset X and is happy with the result.

4.3.2 Data Application and Management ; process (logical) - DAAMS

There are only a limited number of possibilities of overlap between D5.1 (DAAMS) and D8.1 (National Contact Point). After analysis we come to the following four categories:

- No relevant relation between (SOLE/PURE) DAAMS functionality and/or SPE (SOLE/PURE) SPE functionality.
- Relevancy of a DAAMS requirements to the Messaging functionality within the NCP.
- Relevancy of a DAAMS to information processing and messaging for Management Reporting purposes over the HDAB Coordinating Portal (First and Second Line-of-Defence).
- Relevancy of a DAAMS to information gathering and publishing to EU and/or public users for Governance, Risk and Compliance (GRC) reporting to the Board and External Certification Bodies, Auditors and Supervisory entities (Third, Fourth and Fifth line-of-Defence).

Further elaboration of the design will be done in phase II under D8.2. Within the scope of the MVP, the steps are:

1. Implement the messaging service on the NCP.
2. Implement the HDAB Coordinating Portal including Information gathering from the DAAMS and the SPE.
3. Extend the implementation towards processing and dissemination and have HDAB-NL take a decision on Management Reporting functionality.
4. Extend the implementation of the HDAB Coordinating Portal towards GRC Reporting including External Reporting facilities for Supervisory bodies in NL and EU.

Steps 1 and 2 are further explained in the following paragraphs.

4.3.2.1 Step 1. Data permit; application process for a permit (logical)

The following examples help understand the process flow over Corner 1 and Corner 2. This is not a comprehensive list of functionalities over the National Connector within the scope of the Grant Agreement. More designs could follow in phase 2.

Data permit request (*an 'art 68 request'*): apply for data from the EU Data Access Application form

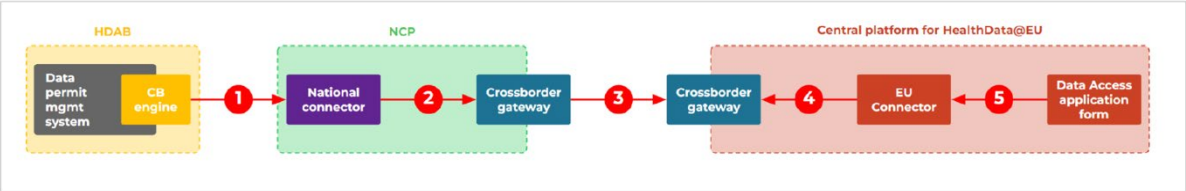


Diagram: Workflow to apply for data from the EU Data Access Application form

1. When a (new) user fills in a data access application form and clicks on submit, the values are sent to the EU connector through a REST-API call. The EU Connector then prepares the eDelivery message (encoding to base 64, authentication to eDelivery) and sends it to the Central Platform Cross Border Gateway.

2. The eDelivery message is sent over the network to the national Cross Border Gateway, leveraging all security features of eDelivery (encryption, authentication).

3. For the data permit, the National connector stores each Data Access Application in a database. It also exposes a REST-API (GET) to read all applications.

4. The Cross-Border Engine is in charge of repeatedly calling the GET-API of the National Connector to import new Data Access Applications into the National Data Permit Management System.

The current implementation for this use case does not yet support a confirmation workflow after the application is received on the national side. This is foreseen as a feature to be added in future releases.

4.3.2.2 Step 2. Data permit; update application process (logical)

Data permit : update application statuses

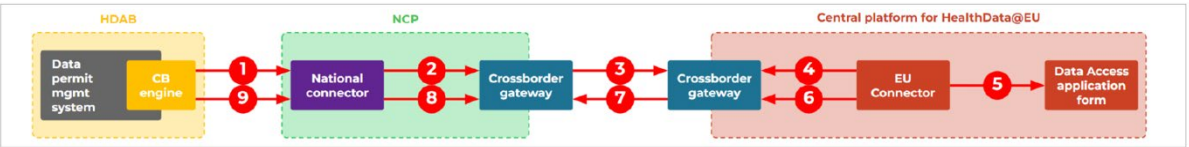


Diagram : Workflow to update application statuses

Implement step 2.

1. The Cross-Border Engine is in charge of identifying when there is a change in the status of the National Data Permit Management System (DPMS). It then calls the APIs of the National Connector with the updated status.

2. For the data permit, the National Connector exposes a REST-API to update the status. When the API is called, the National Connector stores the update in the local database and prepares the eDelivery message (encoding to base 64, authentication to eDelivery) and sends it to the national Cross-Border Gateway.

3. The eDelivery message is sent over the network to the Central Platform Cross-Border Gateway, leveraging all security features of eDelivery (encryption, authentication).

4. The EU Connector reads all eDelivery messages.

5. Once a new data permit message is received, it performs the associated action in the EU Portal.

6. Depending on the success of the operation, the EU connector prepares the eDelivery message (encoding to base 64, authentication to eDelivery) containing the status of the operation and sends it to the central platform Cross Border Gateway.

7. The eDelivery message is sent over the network to the national Cross Border Gateway, leveraging all security features of eDelivery (encryption, authentication).

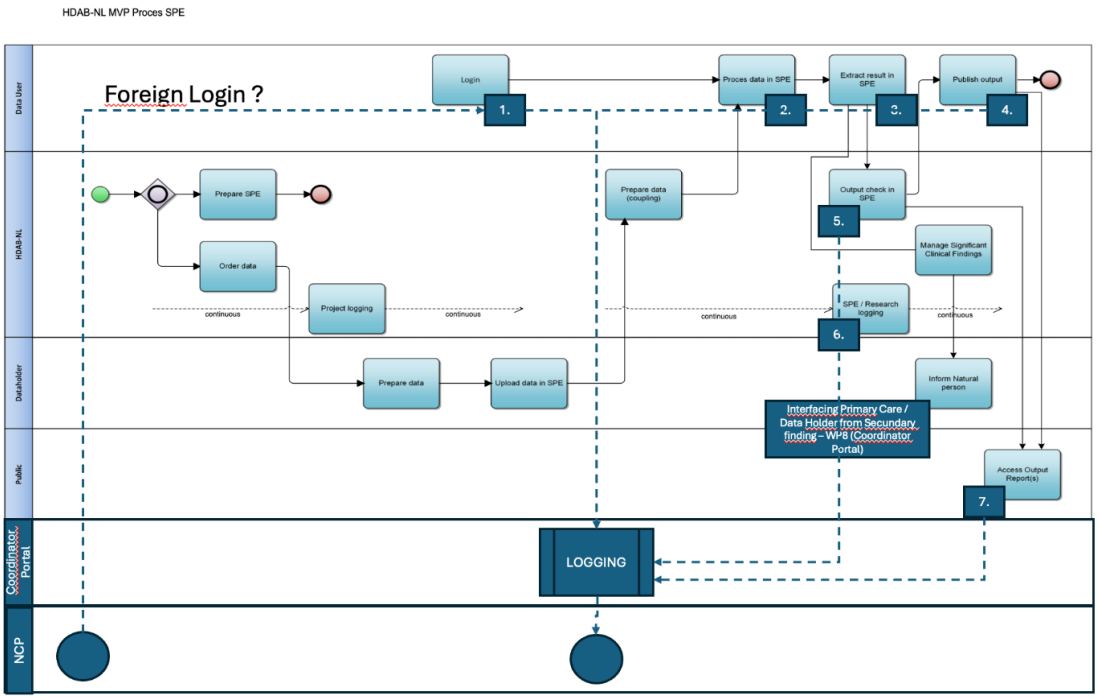
8. That status of the operation is stored in the database of the National Connector.

9. The Cross-border Engine can check the status by calling an API endpoint of the National Connector. If it fails it can raise an alert to the end user managing the national Data Permit Management System.

4.3.3 Data use/utilisation; process (logical) - SPE

WP8 shares some architectural principles with WP7, documented in D7.1 (SPE). The most relevant common requirements are:

- **(Role-based) Access Control**: Strict controls are implemented to ensure that only identified, authenticated, and authorised users have access to the SPE and/or its facilitating infrastructure and only these users can perform authorised actions based on their designated role.
- **Data Protection**: The infrastructural management is set up around Sensitive and/or Highly Sensitive (and valuable) data, so in general policies apply to encrypt and protect from unauthorised manipulation or damage throughout its lifecycle in the entire INFRA, including the infra for the SPE.
- **Monitoring and Logging**: Activity within the infra is monitored and logged in the HDAB Coordinator Portal as well as the Security Architecture and IAM functionality to detect suspicious or unauthorised behaviour and to fulfil the obligations towards data subjects.
- **Interoperability**: The infrastructure supports a localised, regionalised, and centralised or federated approach to data traffic, either over data sets residing at data holders in a central SPE or over a number of different SPE's, through standardisation and interoperability.
- **Usability**: The SPE should be designed with the end-users in mind and effectively support their various use cases and user profiles in an intuitive way. Generic services and Portal UX, including the Messaging Configuration Agent have to be designed, built and setup accordingly.



Diagram; D8.1 provisional events based - SPE process flow

In this diagram, the D7.1 figure 1. (Process for data analysis in SPE) has been linked to the underlying triggers in the event-based architecture (EBA). It is unclear and uncertain as to HOW this EBA should be implemented. Design of the SPE EBA is out of scope for WP8, but links to functionally gathering the utilisation information for

- Reporting management (functional) purposes (Art.59 EHDS).
- Compliance management purposes.
- Audit management purposes.

Further elaboration of the design will be done in phase II under D8.2. The steps are:

1. Log-in into the SPE (as part of Role Based Access to the SPE)
2. Process data in the SPE.
3. Extract results.
4. Output check in SPE.
5. Publish output from the situation of Federated SPE, a Central SPE, a blind central SPE or a Data Preparation Environment (Central SPE for data preparation by HDAB) that is localised, the design and development of the Coordinator Portal of the HDAB may be designed and developed differently.
6. Continuous SPE Research Logging.
7. Access output Reports.

For all these steps applicable governance and security guidelines will be followed. For instance results will be extracted only as aggregated anonimised data. The exact procedures are , however, not in scope of this deliverable.

5 Inventory of the current situation

This approach is as described in the Grant Agreement.

The first step for a successful implementation of the Cross-border gateway solution is to start "Analysis and design" activities. In particular, the analysis and design of the national connector connecting the cross-border gateway to the national infrastructure and the analyses of the overall architecture in general and the generic services in particular.
These activities build upon the outputs from TEHDAS (and in the future TEHDAS2) and upcoming deliverables from Joint Actions on secondary use, as well as on the lessons learned on the HealthData@EU Pilot, to ensure alignment and interoperability with the other HDABs.

The design phase aims to collect a broad set of requirements from a representative cross-section of the data holders, users, researchers, and patients in The Netherlands. The goal of collecting these requirements was to determine success factors for use, acceptance, and governance.

5.1 Analysis and Design-phase

Work plan for WP8 – focusing on the milestones part of D8.1

As a starting point for defining the requirements and specifications for this programme, the available laws and regulations were used. Especially EHDS, NIS2, GDPR, Data Act and Data Governance Act are referenced here.

As a framework for architectural products the tenets of the Open DEI group are used and these have been translated into categories by the Dutch Digilab organisation, a standard widely used and accepted within the Dutch government.

These categories contain subjects found in most governmental projects and will be referred to as RS37 (requirements and specifications; 37 categories) in this document.

After the initial legal requirements (where applicable), the HDAB design principles and values will be used to choose the appropriate standards and/or frameworks for more detailed description of the R&S of the different topics.

A lot of material is already available on most topics. However, often the information is fragmented or applied to a specific use case or scenario.

In the next phase of the programme appropriate standards and solutions will be chosen to satisfy additional functional and non-functional requirements. Where available/obvious, relevant standards have been included in the descriptions of the R&S categories in this deliverable already.

5.2 Outcomes preliminary studies

Several preliminary studies have been conducted to inventory the Current-State-of-HDAB 2024-2025. The following learning points and conclusions can be derived from these studies.

The number of relevant current entities impacted by a National Contact Point is large and the current situation is complex. The impact and the extent to which they will have to accommodate the changes is also quite large. The Dutch data landscape is currently being investigated, though the outcome is not yet known. There are several potential outcomes of the impact of HDAB:

- A centralisation at National level of both the HDAB, as well as its functions such as the National Contact Point
- A federation of Regional and Local Contact Points, under one Coordinating HDAB, that consolidates and manages the Generic Services administration towards the EU
- A Localisation of SPEs at Data Holders and Data Users, with multiple SPEs connected to regionalised, specialised HDAB's with each their own federated (regional) SPE-solutions.
- A combination of the above.

Due to the lack of consolidation in the Netherlands of centralised, national bodies, many of the functions may potentially aggregate or disaggregate over time, depending on the developments in the Dutch healthcare sector. It is uncertain at this point what the future Target infrastructure architecture will look like under these different scenario's.

5.2.1 Starting point of the inventory: the NVS

Current situation of the NL Healthcare sector: Data is limitedly available to others in the care network Dutch care has a multitude of different information systems, portals, platforms and infrastructures. At local, regional, and sometimes national level. Information is now often stored locally under the responsibility of the individual care providers. The exchange of data is often limited to a small number of care providers and is focused on specific applications. As a result, the data can only be used for that specific application. In the current situation, information is missing, which means that providing adequate care and support in the right place and at the right time is not sufficiently facilitated. This leads to extra work and costs and does not benefit the quality of care and support.

The unavailability of health data (such as data from wearables and health apps that contribute to a healthy lifestyle) also hinders citizens in their right to take control of their own health, their own care process, and the way in which data is managed. In the current situation, the citizen cannot get a complete picture of their own health data that is stored in all kinds of systems and can therefore not take control of it. Making data and information available puts the citizen in the position to take control and/or ask others to help with this.

5.2.2 Stakeholder engagement

5.2.2.1 European stakeholder engagement

Community of Practice SG4 establishes the following definition of the cross-border gateway on HealthData@EU side:

The cross-border gateway is a technical construct that provides a common interface for exchanging data. This includes catalogue access and status information on data permits.
The gateway consists of the technical means and security measures to exchange data. It does not describe the format and contents of the data transmitted. In order to have complete functionality, the standardisation of the cross-border communications needs to be augmented with standardisation of the information (semantics, format, encryption) and its interpretation.
The technical properties of the cross-border gateway are described in detail in HealthData@EU documentation. At this stage, the reference model will be followed as proposed by the workgroup.

The current documentation can be found at:
https://webgate.ec.europa.eu/fpfis/wikis/pages/viewpage.action?pageId=2041778671

Collaboration within EHDS2 CoP SG4 and HealthData@EU
WP8 representatives have joined the EHDS2 CoP Subgroup 4 on the Cross-border Gateway. Every three weeks we meet virtually and share developments with the other EU member states. Countries present their governance structures in the health data landscape, user flows for requesting data, specific national challenges, different implementation choices, and interpretations of the EHDS text. In this governance body we also keep track of HealthData@EU developments and tools developed to further develop each national HDAB. Results of the EHDS2-pilot on cross border infrastructure (EHDS2-pilot WP5) have been followed, presented, and discussed to this SG4. The proposed solution by EHDS2-pilot has been improved and is close to being released (including proper documentation). Once released so called connectathons will be organised with national HDABs. Those national HDAB programmes can prepare and deploy their national part of the cross-border gateway before the connectathon is held and ideally, if available test their deployment against the EU (interoperability) test bed to make sure the deployment is successful. This might safe precious time during the connectathons. Once successfully deployed at national side (before or during the connectathon) the connection to the HealthData@EU central part can be deployed/activated and tested. With the SG4-group we collaborate on making scenarios (from simple, e.g. the happy flow of CREATE or UPDATE of a metadata record of dataset X as shown in Diagram of 4.2.3.1; to complex) available for tests over the cross-border gateways.

Collaboration with TEHDAS2.
In Q4 of 2024 the HDAB-NL programme started aligning with TEHDAS2, keeping each other up to date regarding developments within the HDAB-NL work packages and implementing acts resulting from TEHDAS2. In Q1 2025 Nictiz/TEHDAS2 has performed a Wave I consultation of stakeholders that resulted in the following relevant infra requirements:

- Clarified terminology (semantics) should be consistently explained

- Clarified demarcation of (Role Based) Rights by Data holders, data users and HDAB's and SPE's.
- Respondents require consistent use and clear agreements on the use of standards, information models and formats of data descriptions.

To achieve the minimum consistency required by the TEHDAS2 respondents, HDAB-NL uses the RS37 model to standardize the terminology used in all documents and work packages and their individual elements. For more information on RS37, see chapter 7.

5.2.2.2 National stakeholder engagement

A preparatory conference was held in June 2024 to prepare the national kick-off of the HDAB-NL programme. On the 3rd of September, this kick-off was held in Utrecht, with 250+ participants. These consisted of many different origins and organisations to provide a representative cross-section of the healthcare sector and its stakeholders.
The break-out sessions for WP8 had a pre-registration of 50+ participants per session. The outcomes of the sessions were structured based on the RS37 diagram/framework (literally on the floor). Participants were requested to vote by caucus to move to sections they deemed the most relevant/important from their point of view.
The participants in both sessions defined trust and transparency as the paramount outcomes for a future HDAB. To create and maintain trust and support, the overwhelming majority advised to organise governance first and take security and privacy as prerequisite building blocks for further analysis into the HDAB-NL programme. As a follow-up into elaboration of these initial discoveries, HDAB-NL has decided to create a societal advisory council (MAR. maatschappelijke adviesraad) and for the building blocks access to expert council (EG, expert groep) to discuss future requirements and specifications, questions and other issues in more depth with external professionals in the healthcare field.

5.2.2.3 Results of the kick-off of the 3rd of September 2024: Trust beyond infrastructure

The participants of the Kick-Off of the third of September 2024 opted for an infrastructure that will be based on the following principles, foundations, and fundamental building blocks:

Key Principles:

- The data within the “system as a whole” have to be protected on a national level. Preferably with (National) Data Sovereignty as a Key principle – ANY cross-border gateway infrastructure shall be part of that sovereignty on data level.
- The public EN-TRUSTS that the government will PROTECT the data from misuse. Penalties are required and enforcement of compliance as well. The public wants to be able to TRUST BEYOND THE INFRASTRUCTURE
- Generic Services shall be linked to TRUST Services. This requires a TRUST framework approach in the organisational level and a ZERO-TRUST approach on the SECURITY level. This Key principle MAY be implemented on a case-by-case basis based on the Data Confidentiality Level.

Core Values and foundational building blocks:

- The stakeholders require Ethical procedures around the Application of Data Users – This is safe guarded by EHDS. An Ethical-by-design approach is required
- The stakeholders require Privacy-by-design – This is safeguarded by the GDPR, which is applicable to the EHDS.
- The stakeholders require Security-by-design – This must be safeguarded by Security standards that are agreed upon procedures and solutions by the Dutch Healthcare sector. Upon finishing this document no standards have yet been agreed upon, as well no generally agreed-upon procedures have been designed that dictate what the potential HDAB-NL solution architecture will look like, apart from the SPE and General levels of Security required in Dutch Government[11].
- The stakeholders require clear demarcations through Role-Based-Access-by-design. Given the Dutch Healthcare ID system in use (UZI) and the expected Healthcare ID of the future (DIAZ/DEZI-pass) system, it could be reasonably expected that for researchers and healthcare practitioners the RBAC approach will be available. There are no standardised approaches to this on a national level yet for Citizens/Patients (Apart from requirements coming forth from eIDAS and Wdo). The HDAB-Future-board is advised to scan the market on the available solutions in the future.
- The stakeholders require interoperability. This is established by agreements amongst the parties involved and some form of a contract between the department of VWS and the future HDAB-board. No technical solution for interoperability is yet in place. This will have to be designed as of phase II of in the handover process to the future HDAB.

[11] Compliant to Wet Digitale Overheid (WDO) and Wet Beveiliging Netwerk- en Informatiesystemen (WBNI)

6 Requirements and specifications

6.1 Legal requirements EHDS

The final EHDS text has been analysed. The following articles are deemed relevant for D8.1 from the EHDS point-of-view

Subject	Corresponding articles	Chapter and Section
1. EHDS: secondary use of electronic health data	Article 1, paragraph 1 Article 1, paragraph 2, c Article 1, paragraph 2, e Article 1, paragraph 3 Article 1, paragraph 5	Chapter I, Section I - General Provisions
2. **National contact point** for secondary use	Article 75, HealthData@EU; paragraph 1 Article 75, paragraph 3 Article 75, paragraph 4 Article 75, paragraph 6 Article 75, paragraph 7 Article 75, paragraph 8 Article 75, paragraph 11 Article 75, paragraph 12	National Contact Point Par 3: Cross-Border Infrastructure Par 4: Authorized participants Par 6: "... comply with the requirements and technical specifications needed to operate HealthData@EU" Par 7: "...support and facilitate the cross-border access" Par 8:"... Commission shall develop, deploy and operate a central platform for HealthData@EU..." and "The Commission shall only process electronic health data on behalf of the controllers as a processor." "... seek to ensure that HealthData@EU is interoperable with other relevant common European data spaces..." "... Commission shall, by means of implementing acts... a. requirements, technical specifications, and the IT architecture of HealthData@EU b. conditions and compliance checks required to be able to join and remain connected to HealthData@EU c. the minimum criteria that need to be met by the national contact points for secondary use and the authorised participants in HealthData@EU d. common specifications for the architecture of HealthData@EU and for its interoperability with other common European data spaces. The implementing acts referred to in the

		first subparagraph of this paragraph shall be adopted in accordance with the examination procedure referred to in Article 98(2).
	Article 95. Steering groups for MyHealth@EU and HealthData@EU	"...Steering group for for the cross-border infrastructures..."
	Consideration 80 EHDS	Consideration 80: "... bringing questions to data instead of moving those data should be respected whenever possible" Consideration 80: "... authorised participants in HealthData@EU could be (an)... - ERIC: European Research Infrastructure Consortium - EDIC: European digital infrastructure consortium - ESFRI: infrastructures under the European Strategy Forum on Research Infrastructures - EOSC: European Open Science Cloud - Third countries and international organisations could also become authorised participants in HealthData@EU, provided that they are compliant with the requirements in this Regulation (See Art 75, par
	Consideration 105 EHDS	Eu preferences and Technical Specifications on the EU-side are set, mainly based on Open Standards and Open Software reference implementations[12]. They were presented to CoP SG4 – Cross-border Gateway in the course of 2024 in working group meetings. The current central platform technology stack on the central services side is based on a pure-play OS-Software stack. Due to Geopolitical dynamics, this may prove to be an influential strategic direction in which the EU may go. The specifications on standards, as well as the TO BE Software stack on the NL-side are not yet complete and may change due to internal national dynamics. This also true for the TO BE architectural design considerations that are to be initiated through Implementing Acts. The codification and standardisation of EHDS implementing acts may not arrive before 2027. At the moment of finalisation of this D8.1

[12] See: EU Open Source Strategy (and Procurements choices): "Governing Principle, Think Open (5.1) and Stay in Control (5.6) *Open-source solutions will be preferred when equivalent in functionalities, total cost and cybersecurity*", pp. 8; Also "*We promote open standards and specifications that are implemented and distributed in open source*", pp. 10.

		deliverable no version of this deliverable (coming from TEHDAS2) is yet known. The next Wave II stakeholder consultation will be held in sept-2025.
3. Relationship to DAAMS and SPE	Article 57 EHDS: Tasks of health data access bodies	In general: all Art.57, par 1, under a.-k. Requirements apply. Art 57, par 1e "... to record and process health data access applications [not system, but process], health data requests, decisions on those applications and requests and the data permits issued and health data requests handled" - Role based access requirements to the SPE services/capability will be specified under work package WP5 in phase 2. Art. 57, par 1g "... lay down common standards, technical requirements and appropriate measures for accessing [not just process, but also systems access to] electronic health data in a secure processing environment..." - Access requirements to an SPE are specified under work package WP7.
	Article 58 EHDS; Obligations of health data access bodies towards natural persons; paragraph 1	Art 58, par 1 – disclosure of conditions under which EHDS are made available for SU shall be publicly available, easily searchable through electronic means and accessible to natural persons (Also alignment is needed to requirements coming forth out of implementing Wet Open Overheid13 and Wegiz/Information Paragraph14 and Information Standards15 specifically)
	Article 58 EHDS; Obligations of health data access bodies towards natural persons in case of opt-out; paragraph 2	Art. 58, par 2 (in relation to Art.71): " If a Member State has provided for the right to opt out pursuant to Article 71 to be exercised through the health data access bodies, the relevant health data access bodies shall provide public information about the procedure to opt out and facilitate the exercise of that right".
	Article 68, paragraph 11	Art 68, par.11 Alignment between WP8 and WP7 (SPE) is required on Security services
	Article 71, paragraph 1 and 2: Right to opt out from the processing of personal electronic health data for secondary use	Art 71, par 1 and 2: opt-out related functionality and technology, including messaging and storage of communication (The opt-out mechanism shall be accessible and easily understandable for Natural persons – also see our remarks on

[13] See https://www.rijksoverheid.nl/onderwerpen/wet-open-overheid-woo/hoofdlijnen-woo

[14] See https://www.zorginzicht.nl/binaries/content/assets/zorginzicht/algemeen-ondersteuning/handreiking-voor-het-schrijven-van-de-informatieparagraaf-bij-een-kwaliteitsstandaard.pdf

[15] Specifically, the information exchange standards

	Article 73, paragraph 1, a Article 73, paragraph 5 Article 2, paragraph 1 Consideration 29	D10.1). This has impact on Generic services: Identify, Authenticate, Authorise, IF (and only if) this functionality is to be implemented by the HDAB. Art 73, par 1,a: The SPE shall be accessible by natural persons – See WP7 SPE. This has impact on Generic services: Identify, Authenticate, Authorise. Technical, organisational, information security, confidentiality, data protection and interoperability requirements for the SPE-See WP7 SPE. eIDAS shall be used for 'electronic' Identification means Cross-Border eIDAS 'electronic' identification shall be used, regardless of the Natural persons Member State of affiliation.
Identification	Article 67, paragraph 1 and 2 Article 68, paragraph 10 under d.	Art 67, par 2 (application): 1. Natural person Health data applicant's identity 2. Legal Person, Health data applicant's identity, including the identity of the natural persons who would have access to the electronic health data is a data permit were issued. When Legal Person (1 or more people) also: The health applicant shall notify the health data access body of any update of the list of natural persons. The identity of authorised persons, in particular the identity if the principal investigator, with access rights to the electronic health data in the secure processing environment.
Authentication	Indirect (derived from Identity)	When accessing the electronic health data over the portal and into the SPE, the Natural persons are Named Users, and THEREFORE must be AUTHENTICATED by the SPE as BEING the persons PERMITTED to access.
Authorisation	Article 73, paragraph 1 Article 75, paragraph 3, 4, 6, 7 and 12 Considerations 80, 105	The restriction of access to the SPE to authorised natural persons listed in the data permit, issued pursuant to Article 68. Authorised participants (Foundation for Authorisation Generic Service)

Relevant entries for the national contact point can be found at:

- (Art. 75, paragraph 1 and 3) Each country has a national contact point.
- That national contact point for secondary use shall be an *organisational* and *technical (infrastructural)* gateway,
- (Art 55) The national contact point for secondary use may be the coordinator health data access body. Therefore, from an organizational point-of-view the HDAB and the NCP may be the same organization, but EHDS does not enforce this to be so.
- (Art 75, paragraph 8) The Member States and the Commission shall set up HealthData@EU to support and facilitate the cross-border access to electronic health data for secondary use, connecting the national contact points for secondary use and authorised participants in HealthData@EU and the central platform.

Relevant entries for the national connector can be found at:

- (Art 75, par 11) In chapter 5, the HealthData@EU elaboration of the National Connector can be found. In general: every National Contact Point has a National Connector.

In the EHDS only the generic services identification, authentication and authorisation are mentioned:

The Person or Legal person must **Identify** themselves in the application process for the purpose of exactly delimiting the number of persons having access to the electronic health data, once **authorised**.

Identity (Art 67, paragraph 1):

- Natural (one) person, as an applicant
- Legal Person (one or more people), as an applicant

(Art 67, paragraph 2):
When a Legal Person (Rechtspersoon) applies, all “natural persons who would have access to the electronic health data” shall be identified as from the application onwards; also, when this list changes on the side of the applicant, “the applicant shall notify the HDAB of any update of the list of natural persons”;

The principle underlying this listing is identical to a (systems access) Named User Principle, which means that a Concurrent User is not applicable (in theory this can circumvent the delimitation of access and therefore obscure who has access to the electronic health data).

The way of defining the Authentication is derived from the Identification. Due to the delimitation to permitted and listed persons having access, including having to update that list and notify the HDAB, the HDAB has the information to manage the Authentication of that person, or persons, as soon as they access the Electronic Health Data in the SPE. Monitoring and supervision then become part of the process to establish the enforcement of Art 61, paragraph 1 in that: “Health data users may access and process the electronic health data referred to in article 51 for secondary use ONLY in accordance with a data permit issued”.

Identification and **Authentication** mean to identify a natural person through 'electronic means' as defined in EHDS, art 2f and eIDAS (EU 910/2024), art3, points (1) and (2), respectively as: 'electronic identification' and 'electronic identification means':

- 'Electronic identification' means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person.
- 'Electronic identification means' means a material and/or immaterial unit containing person identification data and which is used for authentication for an online service.

Authorisation means to authorise participants to handle health data as defined in article 68, paragraph 5 for the SPE.

6.2 Legal requirements - other relevant sources

Implementing acts of EHDS are expected no sooner than 2027 (in two years). In the meantime it is expected that there will be several other legal and strategic sources applicable, yet there is an inherent uncertainty to the applicability due to the National policies, standards and procedures still missing that have been negotiated or otherwise been laid down as the fundaments of the HDAB-'stelsel' (*system*) in NL. We therefore limit the current list of potentially relevant laws and regulations to a minimum, in order to update this list in the future, as soon as more becomes clear. We mention:

1. EU Data Act
2. EU Data Governance Act
3. Wet Digitale overheid (Wdo)
4. WBNI (NL Data Security – or NIS2 Directive - Cyberbeveiligingswet)
5. GDPR (UAVG)
6. (Future) Interoperability Act
7. (Future) Regulation regarding the utilisation of Open Standards and Open-Source Software for EU based on EU Sovereignty requirements (See: *EuroStack*[16])
8. (Future potential) Regulation regarding the utilisation of software in *Sovereign State Domains/National Digitalisation Strategy*

[16] "The EuroStack initiative presents a bold vision for Europe's digital future, aiming to establish the continent as a leader in digital sovereignty. This comprehensive strategy seeks to foster innovation, strengthen strategic autonomy, and build inclusive partnerships to overcome Europe's reliance on external technologies and position itself at the forefront of the global digital economy". See: https://www.ceps.eu/ceps-publications/eurostack-a-european-alternative-for-digital-sovereignty/

7 Architecture Approach: frameworks

7.1 Requirements and specifications management: RS37

Digilab provides a Dutch governmental framework for categorising subjects in a project. These categories are widely used and accepted and form the basis of structuring the requirement sets within the HDAB-NL programme. The breakdown of categories can be found in the diagram. Since 37 categories have been defined, this framework will be referred to as RS37.

All categories can be found in the following diagram:

Diagram; graphical representation of the RS37 hierarchy and categories

In this diagram you will find four categories of requirements:

1. Trust requirements, which are related to Identity and Access Management Solutions
2. Governance requirements sets that are related to Strategic and Operational requirements for the HDAB organisation
3. Interoperability requirements that are related to interoperability models, traceability of the datasets through catalogues and data services that are required to have the HDAB be operational within the Dutch Data Landscape.

4. And at the end also the ‘value’ components that are related to the ‘why?’ of Trust beyond infrastructure, such as transparency, accountability, and publication of relevant results.

7.2 Elaboration of the RS37 elements

The RS37 categories form the basis of the comprehensive list of requirements, specifications, standards, and agreements that will underpin the working of the initial implementation of the Dutch HDAB. At this stage, some categories have been well defined, others need to still be elaborated on due to the many degrees of freedom that still exist in the choice processes around the HDAB. Not all requirement sets are legally binding. Not all best-practices around certain requirements sets are already applicable to all potential development scenarios. Yet, in the past year all elements of the RS37 framework have been used to create one single set op terminology and architectural ‘vocabulary’, which resulted in consistent studies into the potential development scenarios. The RS37 elements have been studied and analysed on Legal and EU Guideline requirements. Separate, provisional documentation has been prepared by Legal analysts as deepening info on the RS37 set of MVP-requirements for the Netherlands. These Memo’s are separately available to the department of VWS.

For an overview of the place of the RS-elements in the overall framework, you can simply use the RS-reference in the underlying DP8.1 ANNEX-documentation.

8 Conclusion and next steps

As to the current state of uncertainties and subjectivity: the EHDS does not regulate how and by whom all tasks are performed, and obligations are met, how datasets from different sources are combined, how ethical assessments are conducted, how administrative information and health data are exchanged between actors in the ecosystem, or how automated these processes should be. Many of these policy choices are to be made at the national level as they require legislative intervention.

In summary, it is still early to provide policy makers with advice on the optimal policies for a HDAB in the Netherlands. Such an advice would have to be informed by a data landscape analysis[17] as mentioned in D10.1 and a more specific qualification of the good elements of a HDAB as mentioned in the same report. This should come forward through the continuing discovery and experimental work on the national contact point and generic services, sustainability, the data access application management solution, the national dataset catalogue, and the secure processing environment.

Due to the absence of clarity and certainty of implementing act of EHDS, many architectural requirements and options are still open for debate. In the Netherlands, we see a healthcare landscape that has various stages of the formation of local, regional, and national partnerships and in these developments, we noticed different focal points as to the R&S long-term. We can safely conclude that lots of infrastructural options are still open and may actually stay open until a future HDAB organisation has made its choices. This is the prime reason for D8.1 to limit the entire report to what is required by EHDS or other relevant Laws and Regulations, OR report (practically) on what could reasonably be re-used from the existing situation (IST) or be aligned between the Secondary use and Primary use architectural landscape in existing from the perspective of EHDS.

For an HDAB infrastructure, this means that there is still room for multiple scenarios for the future realization of an end-state architecture. The VWS department is currently still investigating the data landscape of the Netherlands as we are finalising D8.1. The outcome of this research and future developments may potentially determine which scenario is realistic for the construction of the first pilots and delivery of the HDAB. No outcome is clear and certain yet at this stage.

Another area of uncertainty is the Solution Architectural strategy. At the finalisation of D8.1 no final decision or even direction of the Solution strategy has yet been chosen or finalized. The Policy compass has yet to be initiated on this. We therefore conclude that it is too soon to report on this entire (technological architectural) layer yet, and this includes any strategic solutions direction of the Application architectural layer in the interoperability model.

[17] D10.1 mentions: ”It is beyond the scope of the work programme of HDAB-NL to do an extensive analysis of the data landscape in the Netherlands. In parallel to the work of the consortium, the Ministry of Health Welfare and Sport has contracted a market research agency as part of its impact assessments in order to prepare for the legislative implementation of the EHDS. These outcomes, when available may also be used by the consortium in order to inform its analyses.” Where such results are available for the next deliverable D10.2, these will be included in D8.2 going forward.

Because there is still so much uncertainty in April 2025, there is still time for the entire sector to come to a joint determination of a policy course for the HDAB. The MVP pilots will start in the coming year. They can certainly contribute to that course determination.

The next steps are therefore to start the (experimental) pilots based on the possibilities that are at hand until the end of the year 2025. For now, starting the pilots and the connectathons is therefore especially important to further involve the stakeholders in this process.

9 Appendix

9.1 Glossary

Accountability	Having accountability means that someone can be described as being liable or answerable for the completion of a certain task. Responsibility can be delegated, but accountability cannot.
Actor	An organisation or an individual performing one or more roles.
Application Programming Interface (API)	A technical interface consisting of a set of protocols and data structuring (API specifications) which enables computer systems to directly communicate with each other. Data or services can be directly requested from a server by adhering to the protocols.
Art	Article
Attribute	Any distinctive feature, characteristic or property of a data object that can be identified or isolated quantitatively or qualitatively by either human or automated means.
Authentication	A process that is used to confirm that a claimed attribute of an entity is actually correct.
Authenticity	In the context of information security, authenticity refers to the truthfulness of information and whether it has been transmitted or created by an authentic sender. Authenticity can be achieved, e.g. by digitally signing a message with the sender's private key. The recipient can verify the digital signature with the matching public key.
Authorisation	The process of giving someone or something permission to do something, for example to gain access to services, data, or other functionalities.
Authorisation Registry (AR)	An authorisation registry manages Records of Authorisation (and, if relevant, Records of Delegation) so that Participants in the Collaborative Solution can verify whether a Data Consumer is authorised to access a specific Data Asset.
Authorisation framework	Overarching framework on how to participate in data spaces, named by the Data Governance Act. See also soft infrastructure
Bilateral Agreement	Covers agreements between two data-sharing actors, ranging from legal obligations to non-binding agreements of principle allowing them to share data.
Business and Policy Components	(e.g., SLAs, business models): These components specify and implement the policies that regulate the exchange and sharing of data between the different actors, on a business level.
CBS	Centraal Bureau voor de Statistiek, Statistics Netherlands
Certificate Authority	A trusted third-party entity issuing digital certificates (e.g. X509-certificates) or host services to validate certificates issued.
Collaborative Solution	A solution in which multiple stakeholders work together to facilitate many-to-many data sharing. The solution can make use of multiple models (i.e. platform and scheme).
Confidentiality	In the context of information security, confidentiality refers to the protection of information from disclosure to unauthorised parties.

Consent	Any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
CPU	Central Processing Unit
Credentials	In the context of information security, credentials are used to control access of someone or something to something, for example to services, data, or other functionalities. The right credentials validate (i.e. Authentication) the identity claimed during Identification.
CRUD	CRUD (acronym for Create, Read, Update, Delete) are considered to be basic functions regarding stored data. In computer programming, possible actions are often mapped to these standard CRUD functions in order to clarify the actions. For example, standard HTTP(S) actions GET and POST refer to Read and Create functions regarding stored data.
DAAMS	Data Access Application Management solution
Data Anonymisation	It is the process of removing personally identifiable information from data sets.
Data application providers	Providers of applications that transform, process, or visualise data.
Data Asset	A data resource, controlled by an organisation to generate revenue, e.g.: a system, application output file, document, database, web page.
Data Consumers	An individual, group, or application that receives data in the form of a collection. The data is used for query, analysis, and reporting.
Data Exchange Board (DEB)	A proposed addition to the Data Innovation Board, which operates on a tactical and operational level.
Data Governance	A system that employs interoperability components (standards and policies) to ensure the acceptable use and high quality of data within a specific ecosystem. Manages the availability, usability, consistency, integrity, and security of the data used.
Data Innovation Board (DIB)	An expert group chaired by the commission. This governance body is foreseen by the Data Governance Act, which operate at a strategic level and advises the Commission.
Data Level Playing field	Competitive landscape has an equal level playing field for all organisations. This means that large monopolistic players can no longer position themselves as exclusive data owners. Data owners regain control and can move between providers. Owning data is no longer the competitive dynamic that decides the winner, and organisations need to offer value to the users to convince them.
Data marketplace	A place where data providers and data consumers can find each other to stimulate data exchange or access.
Data marketplace provider	Provide capabilities that will allow for the operation of data marketplaces.
Data Model	Description of how data can be stored, processed, and accessed.
Data Owners	Entity which has ownership of the data and that has rights to grant or revoke terms and conditions for access and use of data.
Data Permit	means an administrative decision issued to a health data user by a health data access body to process certain electronic health data specified in the data permit for specific secondary use purposes, based on conditions laid down in Chapter IV of this Regulation

Data Pollution	The abundance of data in the digital environment and the damage this can cause to citizens and businesses. It arises from the fact that people and organisations have been giving away massive amounts of data for decades.
Data Portability	The ability of data to be easily moved across interoperable applications and domains. The legal right to data portability, granted in some jurisdictions to individuals, can be delivered through a range of technical mechanisms and varies in scope according to the jurisdiction. Our principle of data portability encompasses the ease of both access to and reuse of data.
Data Producers	Any person, organisation or machine that produces data
Data Providers	Any person or organisation that makes data available.
Data routing and preprocessing (DR&P)	Routing of a data asset to the data consumer
Data Quality	means the degree to which the elements of electronic health data are suitable for their intended primary use and secondary use
Data Quality and Utility Label	means a graphic diagram, including a scale, describing the data quality and conditions of use of a dataset
Data Self-determination	The capacity of an individual or organisation to control who has access to their (personal) data and under what conditions (see also: Data Sovereignty).
Data Set	means a structured collection of electronic health data
Data Set Catalogue	means a collection of dataset descriptions, arranged in a systematic manner and including a user-oriented public part, in which information concerning individual dataset parameters is accessible by electronic means through an online portal
Data Sharing economy (design principle)	Creating the conditions for data trading, which requires a) non-financial incentive mechanisms, b) financial incentive mechanisms, including models to monetize data and methods to determine the value of data, and c) agreements mechanisms.
Data Sharing empowerment (design principle)	Ensuring that decisions can be made by appropriate stakeholders. This means that tools and organisational practices are available for a) governance in data spaces b) citizen engagement support c) data sovereignty support and d) federation.
Data Sharing interoperability (design principle)	Providing the ability for all applications in data spaces to create, use, transfer and effectively exchange data. This requires among other definition of data exchange APIs and data models supporting a) semantic interoperability, b) behavioural interoperability and c) policy interoperability.
Data Sharing publication (design principle)	Enabling data to be published so it can be easily located by data consumers.
Data Sharing trustworthiness (design principle)	Ensuring that data spaces operate according to expected requirements. This means that the development of data sharing applications must support a) security-by-design b) privacy-by-design c) assurance-by-design.
Data Source	A source of data assets that is being exposed to data consumers by data providers. The role responsible for collecting, storing, and controlling personal data which persons, operators, and data using services may wish to access and use.

Data Sources and Services Directory/Catalogue	This directory facilitates dynamic expansion of the data space. Is support dynamic discovery of data processing and data analytic services.
Data Sovereignty	The capability of an individual or organisation to be entirely self-determining with regard to their data (see also: Data Self-determination).
Data space	A data ecosystem, defined by a sector or application, whereby decentralised infrastructure enables trustworthy data sharing with commonly agreed capabilities (data sovereignty and roles).
Data space community (design principle)	Fostering maximum reuse of data space solutions. This includes a) open solutions b) reusability c) open source and d) sustainability of solutions.
Data space engineering flexibility (design principle)	Providing the ability for engineers to add customised features in data processing applications and data platforms to enable a) interoperability flexibility b) trustworthiness flexibility and c) data processing flexibility.
Data Using Service	The role responsible for processing personal data from one or more data sources to deliver a service.
Delegation	The act of designating someone or something to act for another or to represent others. In a data sharing scheme, this means that one party designates another party to share or consume data or to issue authorisations on their behalf.
DPO	Data Protection Officer
Ecosystem	The overall system created by the activities and connections of a set of actors and infrastructure interacting according to a common set of rules. Multiple ecosystems can exist, overlap, and collaborate.
EDPB	European Data Protection Board
EEA	European Economic Area
EHDS	European Health Data Space
eIDAS	An EU regulation on electronic identification and trust services for electronic transactions in the European Single Market. This regulation covers important aspects related to electronic transactions, such as qualified electronic certificates. eIDAS provides a safe way for users to conduct business.
Encryption	Encryption is the process of converting data from plaintext to ciphertext. Plaintext (also called cleartext) represents data in its original (readable) format, whereas ciphertext (also called cryptogram) represents data in encrypted (unreadable) format. Decryption is the process of converting data from ciphertext to plaintext. The algorithm represents the mathematical or non-mathematical function used in the encryption and decryption process. A cryptographic key represents the input that controls the operation of the cryptographic algorithm. With symmetric encryption the same key is use for encryption and decryption, whereas with asymmetric encryption two different, but mathematically related keys are used for either encryption or decryption, a so-called public key, and a private key.
EU	European Union
Federated assurance management	It consists of having individual data spaces assurance management associated with a federated collaboration on a global security and privacy assurance management.

Federated privacy management	It consists of having individual data spaces privacy management associated with a federated collaboration on a global privacy management.
Federated security management	Having individual data spaces security management associated with a federated collaboration on a global security management. Such a framework includes five concepts: identify, protect, detect, respond, and recover. Issues to be addressed include access control, usage control, trust, and identity management.
GDPR	Global Data Protection Regulation (GDPR) is an EU regulation on data protection and privacy, applied from May 25th, 2018. The GDPR's primary aim is to give control to individuals over their personal data and to simplify the regulatory environment for international business.
GDPR	General Data Protection Regulation
Governance	A system of rules, practices, and processes used to direct and manage an ecosystem. A well organised governance needs 3 layers to work in close cohesion: Strategic, Tactical and Operational.
Hard infrastructure	The "tangible" part of the infrastructure, such as roads, rails, cables, but also software components. Elements that everybody who participates in the infrastructure can use.
HDAB	Health Data Access Body
HDAB-NL	Health Data Access Body in the Netherlands (consortium)
HDC	HDAB Health Data Catalogue
HealthData@EU	Cross-border infrastructure as defined in Art. 75 EHDS Regulation
Health Data Holder	means any natural or legal person, public authority, agency or other body in the healthcare or the care sectors, including reimbursement services where necessary, as well as any natural or legal person developing products or services intended for the health, healthcare or care sectors, developing or manufacturing wellness applications, performing research in relation to the healthcare or care sectors or acting as a mortality registry, as well as any Union institution, body, office or agency
Health Data User	means a natural or legal person, including Union institutions, bodies, offices, or agencies, which has been granted lawful access to electronic health data for secondary use pursuant to a data permit, a health data request approval, or an access approval by an authorised participant in HealthData@EU
Health-RI	Health Research Institute, Dutch organisation for research on health data infrastructure
ICTU	Dutch governmental organisation to improve digitalisation of government
Identity Provider	An intermediary party offering services to create, maintain, manage, and validate identity information for parties that share data within a collaborative solution (See also: Collaborative Solution).
Individual	A natural, living human being.
Infrastructure	Build the foundation on which all providers can provide individual services, while still interacting with each other. Infrastructures are sector agnostic. Infrastructures consist of hard and soft infrastructure (see hard and soft infrastructure).

Interoperability	The ability of different systems to work in conjunction with each other and for devices, applications, or products to connect and communicate in a coordinated way, without effort from the person.
Levels of Assurance	Within online authentication, depending on the authentication protocol used, various levels of assurance give the server different degrees of certainty about the client's identity. Depending on parameters such as the quality of the registration process, quality of credentials, use of biometrics or multiple authentication factors and information security, an authentication protocol can provide a server with high or low confidence in the claimed identity of the client. For low-interest products, a low level of assurance might be sufficient, while for sensitive data it is essential that a server is confident that the client's claimed identity is valid.
Metadata	Information about data that helps describe, structure, or administer that data.
MVP	Minimal Viable Product, minimal set of deliverables that provides basic functionality of the complete process (not including all use cases yet)
Non-repudiation	In the context of information security, non-repudiation refers to the fact that the sending (or transmission) and receipt of the message cannot be denied by either of the involved parties (sender and recipient).
Operator	The role responsible for operating infrastructure and providing tools for the person in a human-centric system of personal data exchange. Operators enable people securely to access, manage, and use personal data about themselves as well as to control the flow of personal data within and between data sources and data using services.
Operator Network	A group of operators with some degree of mutual interoperability.
Persistent Identifier	A sequence of characters that identifies an entity, usually in the context of digital objects that are accessible over the internet. Typically, such an identifier is not only persistent but also actionable, i.e. it is a Uniform Resource Identifier (URI), usually of the https type, that you can paste into a web browser to be taken directly to the identified source.
Person	The role of data subject as represented digitally in the ecosystem. Persons manage the use of personal data about themselves, for their own purposes, and maintain relationships with other roles.
PET	Privacy Enhancing Techniques
Pilot	Functional version of the deliverables, containing the complete overall process (see also prototype)
Platform	A platform facilitates the exchange of value between two or more parties, with the multiple parties interacting through the platform.
Platform providers	Provide capabilities that will allow for the operation of (data) platforms.
Policy Administration Points (PAP)	Entity where policies are administered
Policy Decision Points (PDP)	Entity that evaluates access requests that are received from the policy enforcement point (PEP). Subsequently an answer is sent back to the PEP.
Policy Enforcement Point (PEP)	Entity that determines whether an action is permitted or not. It takes any access requests and forwards these to the policy decision point.
Policy Information Points (PIP)	Entity that collects additional (mostly dynamic) information on the data sharing to make accurate policy decisions.

Proto operator	A product, service, or organisation that is in one way or another performing the role of an operator in personal data ecosystems or offers related tools, services, or technologies.
Prototype	Functional version of a deliverable, limited in scope to part of the overall process (see also pilot)
Provenance Data origin.	Role A function or set of responsibilities for a particular purpose.
RIVM	Rijksinstituut voor Volksgezondheid & Milieu, National Institute for Public Health and the Environment
RS	Requirements and specifications
RS37	RS framework derived from Dutch governmental standard
Scheme	A common set of multilateral agreements that facilitates standardised and decentralised data sharing directly amongst participants.
Self-sovereign Identity (SSI)	A model for managing digital identities in which an individual or organisation has sole ownership over the ability to control their accounts and personal data without the need for intervening administrative authorities. SSI allows people to interact in the digital world with the same freedom and capacity for trust as they do in the offline world.
Separation of Concerns (SoC)	A principle by which a modular approach to the development of a system is adopted. This approach entails each section addressing a different aspect (concern) of the overarching system. In the context of SoC in the personal data ecosystem, processing, storing, aggregating, displaying, governing data are concerns that need to be managed in a modular, transparent manner. SoC enables more opportunities for module upgrade, reuse, and independent development.
Soft infrastructure	A soft infrastructure is invisible, made up of technology neutral agreements and standards, on how to participate in an ecosystem. As all participants implement the same minimal set of functional, legal, technical, and operational agreements and standards, they can interact in the same manner independent of the sector or domain.
SPE	Secure Processing Environment
Structured Data Assets	Data that adheres to a predefined data model which is primarily useful for interpretation by machines.
Technical and Technological Components	(e.g., Software, Hardware, Middleware): These components enable the development of the technical solution of a data space. For example, they include devices, network protocols, middleware components and APIs that that enable the exchange of data between different platforms in secure and trustworthy ways.
TEHDAS(2)	(Second) Joint Action Towards the European Health Data Space
Trust Framework	A structure that lets people and organisations do business securely and reliably online.
Unstructured Data Assets	Data that does not have a pre-defined data model or is not organised in a pre-defined way, making it primarily interpretable by humans.
VWS	Ministerie van Volksgezondheid, Welzijn en Sport, Dutch department of Health, Welfare and Sport

Wellness Application	means any software, or any combination of hardware and software, intended by the manufacturer to be used by a natural person, for the processing of electronic health data, specifically for providing information on the health of natural persons, or the delivery of care for purposes other than the provision of healthcare
WHO	World Health Organisation
WP	Work Package within the HDAB-NL project