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: D7.1: SPE: Requirements and Specifications

Starting date of the project: December 1st 2023.

Duration of the project: 4 years (December 1st 2027).

Work package (task): WP7 Secure Processing Environment (SPE – T. 7.1)

Submission date of deliverable: 28th of February 2025

Dissemination level: public

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.

1 Executive Summary

The HDAB-NL project aims at establishing the coordinating Health Data Access Body in the Netherlands together with its supporting digital business capabilities over a four-year period.

Given the sensitivity of electronic health data, data users should have restricted access to such data. Once a data access application for secondary use has been approved, the data or results will be collected and/or processed in a secure processing environment (SPE), in which the results or data are subsequently made available to the data user for the approved use stated in the data permit. A SPE is a highly protected digital workspace where authorised users can analyse health data for purposes defined in the EHDS regulation. It is designed to keep the data safe and ensure privacy by allowing access only to approved users and tools and restricting what can be taken out of the environment, allowing only aggregated anonymised results to be exported.

Several milestones (MS) were developed as building blocks towards this Deliverable 7.1[1] (D7.1); the completion of the analysis and design (T7.1) phase.

- MS 7.1.1: an overview of existing SPE solutions and existing building blocks that could form core components for the final SPE solution(s).
- MS 7.1.2: an analysis of the legal requirements the EHDS imposes on SPE solution(s) of the HDAB-NL, and a comparison with the existing national and international SPE solutions mentioned in the first milestone. Important: the SPE does not have to be one integral system, it can also be a federated system.
- MS 7.1.3: stakeholder analyses. To ensure that the final deliverable 7.1 represents an optimal combination of current SPE-like solutions and new SPE design(s), national stakeholders have been included as early as possible in the process to consult on business and stakeholder requirements.

Despite the delay of business, functional and technical requirements posed by the European Commission, we designed functional components based on prior work and experience developing SPE architectures, both from the Dutch and European SPE landscape. However, it needs to be noted that a future revision of the SPE requirements and specifications when the implementing acts become available is necessary.

Principles on which the SPE architecture were outlined in Chapter 8, as well as the overall business process (Figure 1 – paragraph 8.2). The latter will be supported by the SPE functional components described in paragraph 8.3.

In the SPE landscape under EHDS, there might be one or several types of SPEs, which might differ in their governance structure and functionality. Different types might support different parts of the overarching business process as defined in section 8.2 and there might be differences between the types in the organisations that, fully or in part, fulfil the business roles mentioned in section 8.2. We expect that the mentioned types of SPEs might be part of the SPE landscape under EHDS.

Finally, the component model provides an overview of functional components that can support the overarching business process. The functional components have been identified that together should

[1] A second deliverable (D7.2) will be created containing more sensitive information regarding the SPE which will be limited in its distribution.

cover the entire SPE functionality, for all types of SPEs described in section 8.3. A division has been made between core components that describe the primary processes of the SPE and supporting components that must fulfil the non-functional requirements of the SPEs and span all or most processes supported by the core components.

This deliverable specified the functional legal requirements and specifications for SPEs. In 2025 and 2026, phase 2 will focus on completing this list with business and stakeholder requirements. This also means revisiting this deliverable and, where necessary, aligning with output from TEHDAS2 and HealthData@EU. Subsequently, an MVP will be developed in close coordination with the other technical WPs of HDAB-NL and delivered in August 2026. During phase 2, the WP7 team will keep involving the stakeholder community to ensure the solution(s) is consistent with stakeholder needs and makes a positive impact on research in the Dutch Health Data landscape.

2 Acronyms

Abbreviation	Description
Art	Article
CBS	Centraal Bureau voor de Statistiek, Statistics Netherlands
CPU	Central Processing Unit
DAAMs	Data Access Application Management solution
DPO	Data Protection Officer
EDPB	European Data Protection Board
EEA	European Economic Area
EHDS	European Health Data Space
EU	European Union
GDPR	General Data Protection Regulation
HDAB	Health Data Access Body
HDAB-NL	Health Data Access Body in the Netherlands
HDC	HDAB Health Data Catalogue
HealthData@EU	Cross-border infrastructure as defined in Art. 75 EHDS Regulation
Health-RI	Health Research Infrastructure, Dutch health data research infrastructure
ICTU	Dutch governmental organisation to improve digitalisation of government
RIVM	Rijksinstituut voor Volksgezondheid & Milieu, National Institute for Public Health and the Environment
ODISSEI	ODISSEI (Open Data Infrastructure for Social Science and Economic Innovations) is the Dutch national research infrastructure for social sciences and humanities
PET	Privacy Enhancing Techniques
SPE	Secure Processing Environment
SURF	SURF is the cooperative IT service provider for Dutch education and research institures

Tehdas(2)	(Second) Joint Action Towards the European Health Data Space
VWS	Ministerie van Volksgezondheid, Welzijn en Sport, Dutch ministry of Health, Welfare and Sports
WHO	World Health Organisation
WP	Work Package within the HDAB-NL project

3 Terminology

The EHDS has defined important terminology, which will be applicable for this deliverable. For those definitions not mentioned in Article 2 of the EHDS text, we will use the following interpretation solely for the benefit of this document:

- *Health data access application:*
  An application for a permit to access personal level electronic health data for secondary use as described in article 68 EHDS.
- *Health data access applicant:*
  A natural or legal person submitting a health data access application for a permit ad described in article 68 EHDS.
- *Health data request:*
  A request as described in article 69 EHDS.
- *Health data requestor:*
  Person, institution or public organisation submitting a request as described in article 69 EHDS.

Table of Contents

4 Introduction WP 7: Secure Processing Environment (SPE)

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

The HDAB-NL project aims at establishing 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 carried out by a consortium, consisting of ICTU (coordinator), Statistics Netherlands (CBS), Health-RI 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 (WPs; 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.Given the sensitivity of electronic health data, data users should have restricted access to such data. Once a data application access request for secondary use has been approved, the data or results should be collected and/or processed in a secure processing environment (SPE), in which the results or data are subsequently made available for analysis by the data user.

A SPE is a highly protected digital workspace where authorised users can analyse health data for purposes defined in the EHDS regulation. It is designed to keep the data safe and ensure privacy by allowing access only to approved users and tools and restricting what can be taken out of the environment, allowing only aggregated anonymised results to be exported. Furthermore, the data which is processed within the SPE must not contain any personally identifiable information, which means pseudonymisation and/or anonymisation is necessary. The core aim of an SPE is that the data cannot be physically downloaded by the data user but is analysed within the environment. This guarantees that the use of the data is subject to tight control, which ensures that the data cannot be passed on for unauthorised purposes or linked to other data beyond the underlying data permit. In addition, the data is deleted or archived after the specified utilisation period.

Only individual-level data can exclusively be accessed and analysed within a SPE, whereas aggregated, non-patient level anonymous data is provided of any kind, e.g. via email, as a result of a successful data access request. SPEs are critical to enabling lawful secondary use of personal electronic health data while safeguarding individual privacy and ensuring compliance with EHDS standards. Oversight by the HDAB is essential for a SPE under the EHDS Regulation. Therefore, HDAB-NL will be responsible to ensure regular audits, including by third parties of the SPEs and take corrective actions for any shortcomings, risks or vulnerabilities identified.

To ensure adequate technical and security safeguards for the electronic health data, The Netherlands' Health Data Access Body will ensure access to such a SPE, complying with the high technical and security standards. To meet this aim, this WP on SPE has the following objectives:

- Define practical, technical and security requirements and specifications for secure processing environment (SPE);
- Make an inventory of existing SPE solutions and building blocks that could deliver key components for the final SPE solution(s);

- Design the overarching technical architecture for SPE(s) and create a pilot implementation to be tested with the first use cases;
- Launch an operational secure processing environment for electronic health data.

5 Description of first deliverable

5.1 T7.1 Secure Processing Environment (SPE): Analysis and Design – as described in the Grant Agreement

The first step for a successful implementation of the SPE is to undergo "Analysis and design" activities. While these activities during the first phase of the project officially terminate with this Deliverable 7.1 (D7.1), they will need to be revisited when the outputs from the upcoming Joint Action TEHDAS2 on secondary use become available, as well as more lessons learnt regarding the HealthData@EU Pilot. This is necessary to ensure alignment and interoperability with the other health data access bodies' SPEs. Nonetheless, we expect the results in this D7.1 to not deviate significantly from what TEHDAS2 and the HealthData@EU pilot will deliver and will therefore be an important first stepping stone towards a future final list of requirements and specifications for the SPE of HDAB-NL.

The design phase aims to collect the practical, legal, technical and security requirements from a representative cross-section of the data holders in The Netherlands. We have inventoried the functionalities of existing solutions already operational at CBS (in collaboration with SURF and ODISSEI) and at various Health-RI partners (in particular university medical centres). These solutions jointly already serve thousands of researchers across the Netherlands. This deliverable 7.1 only includes legal requirements for reasons explained later in this document. In phase two, which follows this deliverable, the technical requirements such as size and other characteristics of data files will be inventoried to fit the required IT capacity, administration, logistics processes, staffing and support.

The result will be a detailed design and technical architecture making optimal use of the strengths of CBS and Health-RI, aligned with the requirements of the (second) Joint Action on secondary use and HealthData@EU Pilot. If gaps are identified in this or subsequent phases, it will be considered whether it is useful to add other parties.

6 Approach

6.1 Work plan for WP7 – zooming in on the milestones part of T7.1

Several milestones (MS) were developed as building blocks towards this Deliverable 7.1 (D7.1); the completion of the analysis and design (T7.1) phase.

- MS 7.1.1: an overview of existing SPE solutions and existing building blocks that could form core components for the final SPE solution. The focus here was on the Dutch landscape, but we also looked at advanced systems in the European context. In the future, we will compare our findings with outcomes delivered by the new Joint Action Towards a European Health Data Space (TEHDAS2), HealthData@EU pilot and the Competent Authorities Community of Practice (subgroup 3) in secondary use of health data;

  For now, specifically for this milestone:

  - We shared knowledge between the consortium partners on existing data access portals in the Netherlands;
  - Researched the requirements and specifications from relevant national and international health data access portals;
  - Joined the EHDS2 Community of Practice (subgroup 3) to learn from similar SPE efforts in other European member states;
- MS 7.1.2: an analysis of the legal requirements the EHDS imposes on the SPE solution of the HDAB-NL, and a comparison with the existing national and international SPE solutions mentioned in the first milestone. Important: the SPE does not have to be one integral system, it can also be a federated system. By defining security levels, it can be determined per dataset in which SPE(s) this data may be processed (as part of the Terms of Use). In addition to the SPEs that can be issued by data holders (as the university medical centres and Statistics Netherlands do now), a central organisation may be able to issue SPEs according to the needs of certain use cases or user groups;

  Specifically for this milestone:

  - We learned from our partners working on WP10 about the legal interpretations of the EHDS, the HDAB-NL governance structure, and minimum technical processes which link the technical work packages of HDAB-NL.

- MS 7.1.3: stakeholder analyses. To ensure that the final deliverable 7.1 represents an optimal combination of current SPE-like solutions and a new SPE design, national stakeholders have been included as early as possible in the process to consult on business and stakeholder requirements. These will be further reviewed and included in the following phase; D7.1 only represents the legal requirements for reasons explained below. European stakeholders were those consulted in the EHDS2 Community of Practice (subgroup 3) and the HealthData@EU pilot.

  Specifically for this milestone:

  - We organised an explorative first session to investigate current user journeys and SPE experiences for data holders, researchers, policy makers, IT specialists and other groups, in June 2024;

- We organised two SPE break-out sessions as part of the HDAB-NL kick-off in September 2024 to receive input for requirements and specifications;
- In November 2024 we organised an in-depth technical meeting with business analysts, IT specialists and policy makers from representative stakeholder groups to assess our first reading of legal functional requirements, and asked feedback on business and stakeholder requirements;
- We processed this feedback and comments into the currently presented requirements overview. Business and stakeholder requirements will be further reviewed in the next phase.

6.2 Delays and versioning of requirements

Unfortunately, we have had a slow start due to a slow start on the area of stakeholder involvement and the delay of the final EHDS text, as was already mentioned in Deliverable D.D.1 in December 2024. This means that we could not kick off the HDAB-NL stakeholder engagement fully until September 2024.

Updated versions are to be expected throughout the project when national legislation is adjusted in relation to the EHDS. As mentioned, the new Joint Action Towards a European Health Data Space (TEHDAS2) will come up with implementation acts, which also need to be harmonised with the HDAB-NL and SPE specifically. The same holds for lessons learned in the HealthData@EU Pilot. Finally, lessons learned during the pilot phase, will also make it necessary to keep reviewing the requirements and specifications constantly. In other words, D.7.1 will therefore remain an iterative work in progress.

7 Outcomes preliminary studies

7.1 Milestone 7.1.1: an overview of existing SPE solutions

The landscape of existing SPE solutions and components is complex, both in the Dutch and European context. A complete overview on a European scale is beyond the scope of this document. In Appendix 1 you will find an overview of SPE solutions used in the Dutch context. Appendix 2 provides a mapping table that shows which organisations/use cases use which SPE solutions. Together these appendices provide insight into which solutions are currently available on the Dutch market and how research communities make use of them. These tables aim to create a high-level overview of the SPE landscape and are explicitly not intended to be able to verify whether a described SPE meets a certain set of requirements.

The SPEs are categorised according to different variables. This categorisation was done at a high level to provide insight into the variety of SPEs and how this variation could be suitable for different use cases. The overview includes both central processing environments and federated processing environments. With central analysis, the data user has direct access to the data in a secure environment and can perform the analysis there. With federated analysis, the data remains at the source and the algorithm travels to the data, whereby the data user only receives aggregated results. Hybrid forms also exist, where data are brought into an environment for central analysis, but the data user cannot see the data. Finally, processing environments with secure Multi Party Computation (MPC) offer a way to perform analyses over multiple datasets by means of cryptographic techniques, without sharing the underlying data with each other.

Appendices 1 and 2 show that, although the landscape is fragmented, groups of data holders and data users can be identified who use one or a small number of SPE solutions. For example, within University Medical Centres, anDREa MyDRE is mainly used, supplemented with SURF solutions. In addition to this, various research fields use their own SPE solutions, particularly in an international context and to support use cases that have different functional requirements (for example High Performance Computing - HPC).

7.2 Milestone 7.1.2: EHDS legal requirements for the SPE

Due to the sensitivity of digital healthcare data, access must be strictly limited and controlled so that the data can only be securely processed by authorised persons for the permitted purposes. When a data request for secondary use has been granted, the data must be collected/delivered in an SPE, where the data will then become available for processing.

Naturally, when requesting data (WP 5, DAAMS), a proper assessment will have to be made of the required level of detail (and therefore the level of 'disclosure risk') of data for a specific analysis, whereby the starting point should be that data users are given access to data that do not contain more information than is strictly necessary for the intended processing, both in terms of the number of variables and the aggregation level of those variables. The list of functional requirements below uses the following baseline: the requirements for an SPE in which structured microdata (or record level data) are processed. The requirements formulated from this do not necessarily have to apply to processing data at a higher aggregation level, because the risks of, for example, disclosure of personal data may be non-existent there. Nor do the requirements necessarily apply to processing of other types of data, such as human genetic, genomic and proteomic data. For these special categories of data, while legal requirements still apply, experts will also have to be consulted for the further development of the design. The possibilities of providing synthetic data based on the original data set for processing (a form of randomisation) are also not discussed, although it should of course be noted that there are opportunities in this area to organise the processing of sensitive data in a more secure manner. Within the SPE, in the case of processing microdata (or record level data), the data protection and privacy protection measures must meet the highest possible standards, without hindering the processing for the intended purpose.

In sum, health data access bodies shall provide access to electronic health data pursuant to a data permit only through a secure processing environment which is subject to technical and organisational measures and security and interoperability requirements (article. 73, paragraph 1, EHDS, Nov 27, 2024):

1. Access to the secure processing environment is restricted to authorised natural persons listed in the data permit issued pursuant to Article 68 (article. 73, paragraph 1, a, EHDS, Nov 27, 2024).
2. The health data user only has access to the electronic health data covered by their data permit. This is ensured by:
   - giving the authorised natural persons listed in the data permit individual and unique user identities;
   - setting up confidential access modes (article 73, paragraph 1, d, EHDS Nov 27, 2024).

3. SPE must minimise the risk of the unauthorised reading, copying, modification or removal of electronic health data hosted in the secure processing environment through state-of-the-art technical and organisational measures (article 73, paragraph 1, b, EHDS, Nov 27, 2024).

4. Access is only provided to electronic health data that is adequate, relevant and limited to what is necessary in relation to the purpose of processing in line with the data permit. The HDAB shall provide electronic health data in an anonymised format, where the purpose of processing by the health data user can be achieved with such data. Access to electronic health data in pseudonymised format is only provided where the health data user has sufficiently demonstrated that the purpose of processing cannot be achieved with anonymised data in accordance with Article 68(1), point (c). (article 66, EHDS, Nov 27, 2024).

5. The SPE complies with the following security measure: the SPE limits the input of electronic health data, and the inspection, modification or deletion of electronic health data hosted in the secure processing environment to a limited number of authorised identifiable individuals (article 73, paragraph 1, c, EHDS Nov 27, 2024).

6. Identifiable logs of access to and activities in the secure processing environment are maintained for the period necessary to verify and audit all processing activities in that environment. Access logs shall be kept for at least one year (Article 73 paragraph 1 e, EHDS Nov 27, 2024).

7. SPE ensures compliance and monitors the security measures to mitigate potential security threats (Article 73 paragraph 1 f, EHDS Nov 27, 2024).

8. Health data access bodies shall ensure that electronic health data from health data holders in the format specified in the data permit can be uploaded by those health data holders and can be accessed by the health data user in a SPE (Article 73 paragraph 2, EHDS Nov 27, 2024).

9. Health data access bodies shall review the electronic health data included in a download request to ensure that health data users are only able to download non-personal electronic health data, including electronic health data in an anonymised statistical format, from the secure processing environment (Article 73 paragraph 2, EHDS Nov 27, 2024).

10. By … [two years from the date of entry into force of this Regulation], the Commission shall, by means of implementing acts, lay down the technical, organisational, information security, confidentiality, data protection and interoperability requirements for the secure processing environments, including with regard to the technical characteristics and tools available to the health data user within the secure processing environments (Article 73 paragraph 5, EHDS Nov 27, 2024).

The next chapters will build further on this first baseline analysis.

7.3 Milestone 7.1.3: national and international stakeholder engagement

7.3.1 National stakeholder engagement

In June of 2024, we organised a stakeholder meeting to help us map out current (without an existing HDAB-NL) user flows and journeys per stakeholder group (researchers, data holders, policy makers, medical staff, IT specialists, private sector, patient representatives). This meeting provided us with valuable information on the current reality of these stakeholder groups in the Dutch fragmented health data landscape. During this session, however, we could not explicitly ask about business and stakeholder requirements for the future HDAB-NL and SPE for political reasons.

The latter happened during two break-out sessions of the official national HDAB-NL kick-off in September 2024. For this interactive session we identified eight thematic components within the user journey, so that during the session we could ask for input on desired functionalities within each component. Participants were also asked to sign up for our online community to contribute further if desired. We digitalised all input and incorporated it in the first draft of the requirements and specifications.

Mid November 2024 we held an in-depth workgroup session with a small group of dedicated external stakeholders to review the legal requirements we had defined based on the first version of the EHDS 7.1.1. This only represented one third of the sources for the requirements; the business and stakeholder requirements were not included. For the latter we identified a second list and asked stakeholders to participate in a prioritisation and feedback exercise. Many valuable insights were provided, and these will be further incorporated in the subsequent phase of this project, after submission of D7.1.

7.3.2 Collaboration within EHDS2 CoP SG3 and HealthData@EU

We have joined the EHDS2 CoP Subgroup 3 on the SPE. 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.

7.3.3 Collaboration with TEHDAS2

In Q4 of 2024 we started closely aligning HDAB-NL with TEHDAS2, keeping each other up to date regarding developments within the HDAB-NL working packages and implementing acts coming out of TEHDAS2.

8 SPE architecture and requirements

8.1 Architecture principles for SPEs

The EHDS regulation states that health data must be processed in a secure processing environment. The current document poses the legal requirements for such an environment, based on the most recent version of the regulation (January 2025). Business requirements, functional requirements and technical requirements greatly depend on the implementing acts currently being developed by other European governance bodies like Tehdas2 and HealthData@EU. This means the list currently presented will need to be revisited when the implementing acts are published.

Despite the delay of business, functional and technical requirements posed by the European Commission, we can design functional components based on prior work and experience developing SPE architectures, both from the Dutch and European SPE landscape. However, it needs to be noted that a future revision of the SPE requirements and specifications when the implementing acts become available is necessary.

The SPE architecture will be based on the following principles:

- Isolation: The secure processing environment is separated from other environments, and projects within the secure processing environment are isolated from each other to prevent unauthorised access or interference.
- (Role-based) Access Control: Strict controls are implemented to ensure that only authorised users have access to the SPE and only these users can perform authorised actions based on their designated role.
- Data Protection: Sensitive data is encrypted and protected from unauthorised manipulation or damage throughout its lifecycle within the SPE.
- Monitoring and Logging: Activity within the SPE is monitored and logged to detect suspicious or unauthorised behaviour and to fulfil the obligations towards data subjects.
- Interoperability: The SPE supports a central or federated approach to data analysis, 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.

8.2 SPE overarching business process

The overall business process (Figure 1) should be supported by the SPE functional components described in paragraph 8.3. Roles and responsibilities have not yet been assigned throughout the entire business process, since they have not been determined yet.

Precondition

- The health data user has submitted a health data access application through the DAAMS process and the HDAB has issued a data permit pursuant to Article 68.
- The SPE conforms to the HDAB requirement framework and can thus be used to process the data stated in the data permit.

Trigger

- The DAAMS instructs the data holder to make the requested data available in the appropriate SPE.

Conceptual process model

1. The SPE operator provisions and configures the SPE as requested by the data user in their data access application.
2. The SPE operator installs the necessary software in the SPE.
3. The data holder compiles the requested dataset in a minimised form, including only the data that are needed for the proposed project, as detailed in the data permit.
4. The data holder consults the opt-out registry to suppress data in the dataset for which appropriate consent is lacking (if necessary).
5. The authorised role (HDAB, data holder or third party) pseudonymises the requested dataset (if necessary).
6. The data holder makes the data available for processing in the SPE[2] (for the duration agreed in the data permit).
7. The SPE operator gives the data user authorisation to access the SPE using the generic Identification, Authentication & Authorisation (IAA) service.
8. The data holder notifies the HDAB that the desired dataset has been made available, so that the status of the request can be updated.
9. The data user accesses the SPE through the generic IAA service.
10. The data user performs the analysis on the input data and generates analysis results.
11. The data user requests export of analysis results.
12. The authorised role (HDAB in case of central analysis or data holder in case of federated analysis) checks the analysis results for the disclosure of personal data and approves or rejects the export request.

[2] The type of processing determined in which SPE the data provider makes the data accessible. This is further explained in paragraph 7.3.2 Data Provisioning.

13. The SPE operator makes the analysis results available for the researcher.
14. The authorised role (HDAB in case of central analysis or data holder in case of federated analysis) makes the data preparation and analysis workflow available in a trusted software repository.
15. The data user has completed the data processing and the SPE operator cleans up the SPE (removal of all health data and other research files).

Postcondition

- The data has been processed, and the results have been secured.
- Any linked and/or enriched data have been secured.
- The secure processing environment has been cleaned up.
- The study is documented in such a way that the results can be reproduced.

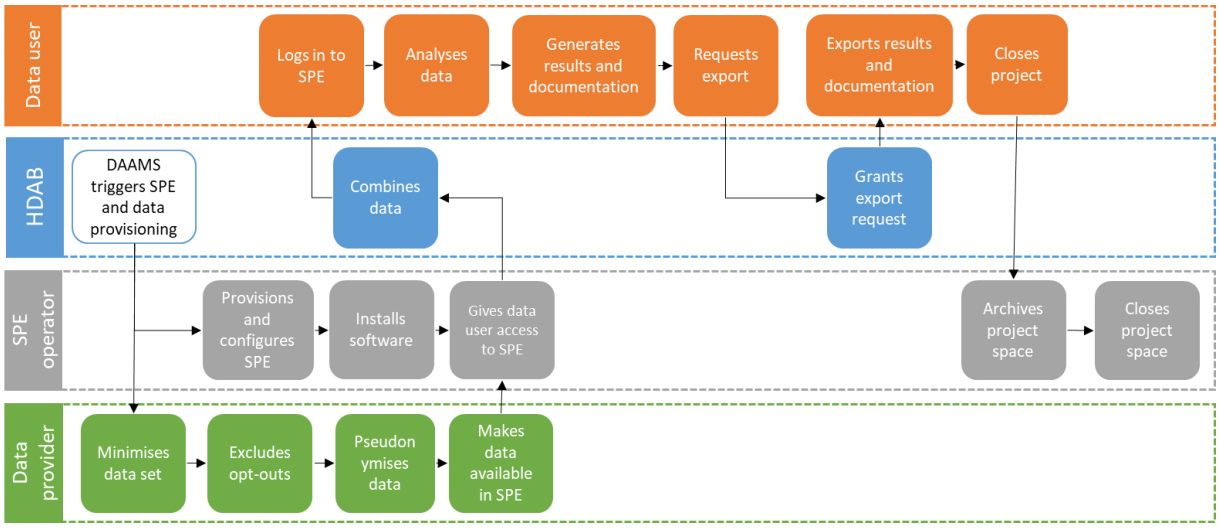

Figure 1. Process for data analysis in SPE

8.3 Types of SPE and their application in EHDS architecture

In the SPE landscape under EHDS, we expect several types of SPEs, which might differ in their governance structure and functionality. These different types might support different parts of the overarching business process as defined in section 8.2 and there might be differences between the types in the organisations that, fully or in part, fulfil the business roles mentioned in section 8.2. We expect that the following types of SPE's might be part of the SPE landscape under EHDS. Below, each of these types is described in detail.

- Federated SPE;

- Central SPE;
- Blind central SPE;
- Data Preparation Environment (Central SPE for data preparation by HDAB).

Federated SPE: In federated SPE systems, the data are processed at the source and the analysis travels to the data. One of the nodes in a federated system serves as an aggregator, where results from different data holders are securely combined before release to the data user. If the aggregation of results involves linking record-level data, this needs to be done in a secure environment.

Central SPE: In central SPE systems, pseudonymised data are brought together in one environment for processing. The term “central” refers to the fact that data are combined in one environment. This central SPE does not need to have central governance and could for example be located at a data holder. The data user can see and “feel” the data during the analysis.

Blind central SPE: In a blind central SPE, data are also brought together in the same environment, but the data user cannot see the data but can only interact with the data by sending the analysis to the environment. In cases where a single data set is processed at the environment that is under the governance of the data holder, the governance is similar to that of federated analysis.

Data Preparation Environment: HDAB will provide a trusted data preparation environment, not accessible to data users, where requested data can be received from data holders and combined, prepared, and pseudonymized before it is made available in an SPE. This environment might be used in cases where data from more than one data holder needs to be combined without giving the data user access to the linking keys or pseudonyms.

Section 8**Fout! Verwijzingsbron niet gevonden.**4 will describe any differences in architecture or governance between these types of SPE on the level of the functional components.

8.4 Component model

The component model provides an overview of functional components that can support the overarching business process. The functional components have been identified that together should cover the entire SPE functionality, for all types of SPE described in section 8.3. A division has been made between core components that describe the primary processes of the SPE and supporting components that must fulfil the non-functional requirements of the SPE and span all or most processes supported by the core components. Note that the component model was developed based on the expected functionality, while detailed functional requirements have not yet been defined. In this deliverable, we define legal requirements and the functional components as well as the core processes they should support are still under development.

The components displayed below in grey have a relation to the SPE environment's core components but are not covered in this document.

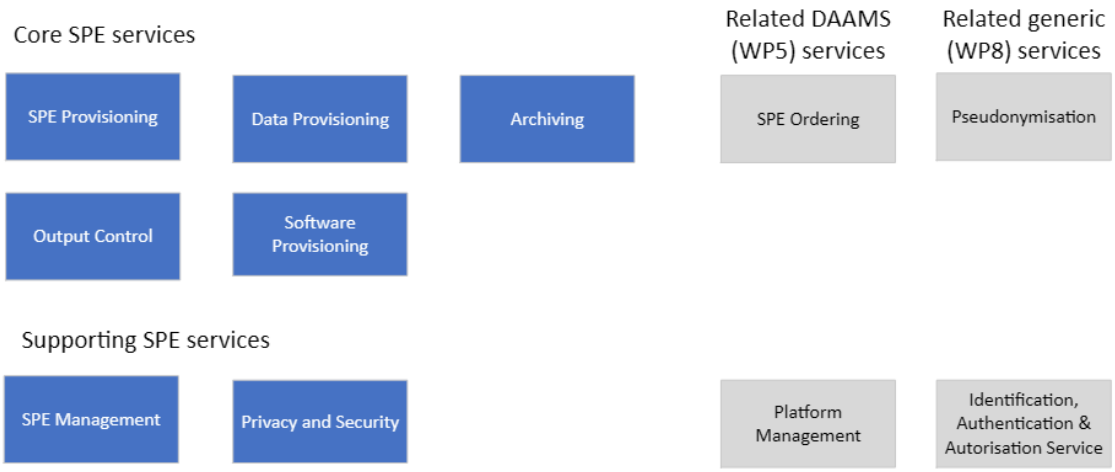

Figure 1: Component model defining the functional components of the SPE. Note that the reference to system or application in this document does not indicate a specific solution. A solution can cover the functionality of one or more core- and/or supporting services.

In the following sections, the **SPE core components** and **SPE supporting components** will be described in more detail and the most important legal requirements and business processes for each component will be described. The **SPE core components** are described in section 8.4.1 and the SPE Supporting Components are described in section 8.4.2.

8.4.1 SPE Core Components

8.4.1.1 SPE Provisioning

In SPE Provisioning processes are described that prepare the SPE for data processing and allow the data user to interact with the SPE and process the data. This entails giving the SPE access to the appropriate compute and storage resources, configuring the appropriate roles and authorisations, and in case of a federated SPE, configuring the connections with data holder SPE's for federated analysis.

This system supports the following core processes:

- Provisioning and configuring the SPE as requested by the data user;
- Configuring the appropriate roles and authorisations in the SPE, according to the data permit;
- Giving the SPE access to the necessary compute capacity;
- Giving the SPE access to the necessary storage capacity;
- In case of federated network configuration: enabling secure and compliant connections to data holders' systems for analysis (without centralising data).

Configuring the SPE as requested by the data user entails a process that either uses information from the DAAMS or allows for interaction between the SPE operator and the data user. Use cases for secondary use of health data vary widely and pose different requirements on the SPE configuration, for example:

- Data set size poses requirements on storage and compute capacity, ranging from a CPU to High Performance Computing (HPC);
- Analysis complexity also poses requirements on compute capacity;
- Connections to reference data sets might be needed;
- Data user might need or prefer a specific operating system;
- The SPE might need configuration to function as a node in a federated network.

There are no legal requirements linked to this component as the EHDS does not pose legal demands on SPE provisioning.

8.4.1.2 Data Provisioning

Data Provisioning is the process of creation, preparation and enablement of a network or system to provide data from data holder(s) to the HDAB data user.

An SPE might be configured as a Data User SPE (central or federated) or as a Data Preparation Environment. A Data Preparation Environment provides largely the same functionalities as any SPE but is placed fully under governance of the HDAB. This environment functions as an "internal SPE" for the HDAB and allows the HDAB to prepare and combine data from different data holders before the final data set is made available for processing by the data user.

This system supports the following core processes:

- Securely connecting to and/or receiving data from data holders (for central systems and Data Preparation Environment);
- Securely storing data for use in the SPE (for central systems and Data Preparation Environment);

- Establishing a secure connection between the SPE and possibly other SPEs (in case of federated systems);
- Combining, preparing and compiling data (for Data Preparation Environment).

The following requirements are part of this component:

- **Requirement 1.003:** HDAB shall ensure processing of electronic health data such as the receiving, combining, preparing and compiling of necessary requested data from health data holders, the pseudonymisation or anonymisation of the data (EHDS article 57 par. 1 b).

  Business process for this requirement: Data is prepared, combined and pseudonymised/ anonymised by HDAB or the data holder before it becomes available to the data user in the SPE.

- **Requirement 1.004:** HDAB ensures that data are available for the data user within the SPE only for the time period stated in the data permit. (EHDS art. 68 par 10 sub e and par 12.)

  Business process for this requirement: Access to SPE is managed by permit information from DAAMs.

- **Requirement 5.016:** HDAB ensures that data from data holders can be uploaded in a secure way by the data holders to the SPE (EHDS art. 73 par. 2).

  Business process for this requirement: The SPE provides secure data import from data holder or trusted data exchange solution.

- **Requirement 5.019:** HDAB shall provide a mechanism for data holders to upload data to the SPE in the format determined by the data permit (article 73 par. 2).

  Business process for this requirement: The SPE provides data import, allowing all requested/agreed data formats.

8.4.1.3 Software Provisioning

Software Provisioning ensures that data users have access to the tools they need to analyse data within the SPE. This component involves the installation, configuration and maintenance of software applications that users require to carry out their analyses. The software can either be standard tools pre-installed by the SPE operator or custom tools preferred by data-users. This process includes managing software licenses, ensuring version control and facilitating secure software updates. In federated SPEs, software (both to set up the federated analysis infrastructure and to analyse the data) might need to be provisioned to the data holder SPE(s).

This system supports the following core functions and processes:

- SPE software installation: installing and configuring analytical tools and applications required for research projects;
- Software license management: ensuring compliance with software licensing agreements for both standard and user-requested tools;
- Software version control;

- Secure software import from trusted repositories: allowing users to download additional tools securely from trusted sources without compromising system security.
- Secure software upload to trusted repositories: allowing users to share their custom-built tools or pipelines with trusted sources without compromising system security.

There are no legal requirements linked to this component as the EHDS does not pose legal demands on software provisioning. See section 8.4.1.4 for requirements surrounding any (software) exports from the SPE and section 8.4.2.2 for security requirements, which also encompass software management in the SPE.

8.4.1.4 Output Control

Output Control is the process that allows the data user to prepare the achieved output for export and the HDAB to verify that the output does not contain personally identifiable data. In this component, the assessment takes place to see whether security and privacy regulations are adhered to and whether the data fulfils all requirements for export. In federated systems (including MPC) output control is performed on results that are to be released to the data user from data holder SPEs and/or a secure aggregator SPE.

This system supports the following core processes:

- Prepare output data for export (data user);
- Prepare output scripts or tools for export (data user);
- Review of output data to ensure non-identifiability; checking analysis results to ensure they do not include personally identifiable information and reviewing and approving results before they are shared outside the SPE (HDAB);
- Review of output scripts or tools do not include personally identifiable information (HDAB);

The following requirements are part of this component:

- **Requirement 5.010:** HDAB shall ensure by reviewing that the health data users can only download non-personal electronic health data, including electronic health data in an anonymised statistical format and output scripts from the secure processing environment. (article 73 par. 2).

  Business process for this requirement: Output data is checked for personal electronic health data.

8.4.1.5 Archiving

Archiving is the functional component organising and performing the archiving of the contents and properties of an SPE, including the query for the creation of the requested data set, analysis scripts and pipelines, associated metadata, and SPE settings. Archiving should ensure that all components are safely preserved for future validation and reproducibility. This is necessary to ensure that results can be validated and reproduced for good scientific practice and for compliance of HDAB with European and national legislation (Archive Law and EHDS). **This system supports the following core processes:**

- Securely archive linked or enriched data;
- Securely archive analysis;
- Securely archive SPE settings, including installed software with versions.

The following requirements are part of this component:

- **Requirement 1.001:** HDAB shall ensure that the formula for the creation of the requested data set is preserved after termination of the research, in accordance with the applicable European and national laws. (EHDS art. 68 (12), art. 87)

  Business process for this requirement: Upon completion of research in an SPE, data, queries, scripts, pipelines and SPE settings and metadata are stored for a fixed period of time, so that they remain available for future reproduction and analysis.

8.4.2 SPE Supporting Components

Each **supporting component** is described below. The supporting capabilities consist of non-functional processes and functions that support the SPE core application components and generic services.

8.4.2.1 SPE Management

SPE Management entails the processes needed to maintain the SPE and manage its resources. Furthermore, SPE management facilitates auditing and certification. Requirements of SPE management apply to all SPE types.

This system supports the following core functions and processes:

- SPE resource management: monitoring and adjusting system resources like storage and computing power, to keep the SPE running efficiently;
- SPE maintenance: performing regular updates, fixing issues, and improving system performance to keep the SPE secure and reliable;
- SPE documentation: providing user documentation and documentation to support auditing, keeping documentation up to date;
- SPE support: providing data user and data provider support, including receiving, handling and reporting back on user issues and questions;
- SPE auditing: regularly checking the system to ensure it follows all technical, legal, and operational requirements for certification.

The following requirements are part of this component:

- **Requirement 2.001:** Identifiable logs of access to and activities in the secure processing environment are maintained for the period necessary to verify and audit all processing activities in that environment. Access logs shall be kept for at least one year (Article 73 par 1 sub e).

  Business process for this requirement: Logging of: 1. access to the SPE by data users, 2. input and output to and from the SPE and 3. activities within the SPE. Retention of these logs for a minimum period not shorter than one year.

- **Requirement 5.020:** HDAB shall ensure regular audits, including by third parties, of the secure processing environments and shall take corrective action for any shortcomings, risks or vulnerabilities identified by those audits in the secure processing environments (article 73 par. 3).

  Business process for this requirement: The system supports regular audits, including external audits, to ensure compliance with operational and security requirements.

- **Requirement 5.021:** HDAB shall ensure that the SPE managed by HDAB as well as 3rd party SPEs that are certified and approved to be operated within the HDAB environment will conform to all statutory regulations. (EHDS art 73 E, art. 57 par. 1 sub a under i)

  Business process for this requirement: HDAB ensures that all SPEs within HDAB meet legal, technical and operational requirements for certification.

- **Requirement 6.010:** HDAB implements requirements following from implementation acts adopted by the European Commission, specifying technical, organisational, information security, confidentiality, data protection and interoperability requirements for the secure processing environments, including the technical features and tools available to the user of health data in the secure processing environment. (EHDS art 73 par 5)

  Business process for this requirement: Processes regarding requirements following the implementation acts.

8.4.2.2 Privacy and Security

The Privacy and Security component ensures that all data and activities within the SPE meet the highest levels of security and privacy protection. This includes implementing strict access controls, monitoring for potential security threats, performing regular penetration tests and ensuring compliance with regulations such as GDPR. Emergency protocols are in place to respond to incidents effectively. The Privacy and Security component interacts with all other components of the SPE and is applicable to all types of SPE.

This system supports the following core functions and processes:

- Managing user authentication and access controls: verifying user identities and ensuring only authorised users can access the system;
- Protecting sensitive data: keeping data secure using technical measures such as secure storage systems and encryption;
- Protecting the privacy of data subjects using technical and organisational measures such as PETs, anonymisation and screening input data for identifiable information;
- Monitoring for security risks: continuously checking for risks and taking action to mitigate them;
- Responding to incidents: quickly responding to (by lock-down) and resolving security issues.

The following requirements are part of this component:

- **Requirement 4.7:** HDAB must ensure that the security and infrastructure of the SPE is audited based on European standards supplemented with national standards. HDAB must provide HDAB managed Secure Processing Environments (SPEs). HDAB must provide a certification track for 3rd party managed secure processing environments (SPE). (EHDS art 73 par 3)

  Business process for this requirement: HDAB ensures robust security and compliance by auditing the SPE infrastructure against European and national standards. HDAB provides secure environments for data processing while enabling third-party SPEs to be HDAB-certified.

- **Requirement 5.004:** SPEs shall minimise the risk of the unauthorised reading, copying, modification or removal of electronic health data hosted in the SPEs through state-of-the-art technical and organisational measures. (EHDS art 73 par 1 sub b).

  Business process for this requirement: The SPE is designed with only authenticated access for persons and data as stated in the permit, and with controls on outgoing data. The risk of unauthorised access to or manipulation of the data is minimised.

- **Requirement 5.005:** Staff authorisation to enter SPE is based on access by necessity (EHDS art 73 par 1 sub c).

  Business process for this requirement: The SPE is set up with a management option with limited access for administrators. Record the reason for access.

- **Requirement 5.006:** HDAB will only grant access to the SPE to the authorised natural persons listed in the respective data permit (EHDS article 73 par 1 sub a).

  Business process for this requirement: The SPE only grants access to the authorised natural persons listed in the respective data permit.

- **Requirement 5.007:** HDAB must ensure that health data users have access only to the electronic health data covered by their data permit, by means of individual and unique user identities and confidential access modes (article 73 par 1 sub d).

  Business process for this requirement: In the SPE health data users only have access to the electronic health data covered by their data permit.

- **Requirement 5.014:** HDAB ensures that data in the SPE is adequately pseudonymised or anonymised, in accordance with the data permit (EHDS art 66 par 3).

  Business process for this requirement: Data within the SPE must be sufficiently anonymised or pseudonymised.

- **Requirement 5.017:** HDAB will ensure emergency protocols are available for a general lockdown of the HDAB platform and SPE in case of security issues, data leaks or other high impact incidents or risks. Initiating a lock down can be requested by security officers in which case the SPE operators execute the workspace(s) (temporary) lock down.

  Business process for this requirement: The SPE management plan includes a disaster preparedness plan, in which the SPE environment can be made completely inaccessible in the event of a serious incident.

- **Requirement 6.005:** HDAB shall ensure compliance with, and monitoring of the security measures referred to in EHDS art 73 par 1 to mitigate potential security threats. (EHDS art 73 par 1 sub f)

Business process for this requirement: The safety measures surrounding the SPE are monitored.

- **Requirement 6.008:** HDAB shall ensure the SPE managed by HDAB as well as 3rd party SPEs are GDPR compliant. (EHDS art 77 (consideration), EHDS art 74)

  Business process for this requirement: Controlling and ensuring data access and data transfers are GDPR compliant.

9 Conclusion and next steps

A SPE is a highly protected digital workspace where authorised users can analyse health data for purposes defined in the EHDS regulation. Research-, personal and other healthcare related data can exclusively be accessed and analysed within an SPE, whereas aggregated, non-personal level anonymous data is provided by any means, e.g. via email, as a result of a successful data access request. SPEs are critical to enabling lawful secondary use of personal electronic health data while safeguarding individual privacy and ensuring compliance with EHDS standards. Oversight by the HDAB is essential for an SPE under the EHDS Regulation.

In order to ensure adequate technical and security safeguards for the electronic health data, The Netherlands' Health Data Access Body will ensure access to such a SPE, complying with the highest technical and security standards. To meet this aim, this WP on SPE has the following objectives:

- Define practical, technical and security requirements and specifications for secure processing environments (SPE);
- Make an inventory of existing SPE solutions and building blocks that could deliver key components for the final SPE solution;
- Design the overarching technical architecture for the SPE and create a pilot implementation to be tested with the first use cases;
- Launch an operational secure processing environment for electronic health data.

This deliverable specified the functional legal requirements and specifications for the SPE. In 2025 and 2026, phase 2 will focus on completing this list with business and stakeholder requirements. This also means revisiting this deliverable and, where necessary, aligning with output from TEHDAS2 and HealthData@EU. Subsequently, an MVP will be developed in close coordination with the other technical WPs of HDAB-NL and delivered in August 2026. During phase 2, the WP7 team will keep involving the stakeholder community to ensure the solution is consistent with stakeholder needs and makes a positive impact on research in the Dutch Health Data landscape.

10 Appendices

In addition to the overview of available solutions, this table provides some insights into which data holders and data users in the current landscape use the different SPE solutions.

10.1 Appendix – Legal requirements and their business processes

Req. ID	Req. Title & Description	Business components	Business Process	Functional Requirement Description	Articles of Law
WP7-REQ-1.001	HDAB shall ensure that the formula for the creation of the requested data set is preserved after termination of the research, in accordance with the applicable European and national laws. (EHDS art. 68 (12), art. 87; Archiefwet)	Archiving	Upon completion of research in an SPE, data, queries, scripts, pipelines and SPE settings and metadata are stored for a fixed period of time, so that they remain available for future reproduction and analysis.	The system will provide the functionality to store finalised and disseminated research including any research papers, summarised data (statistically secured) and associated methodology. Within case management a completed research project can be archived including the research results as described above. - Archive case; - Attach research results to case; - Browse, search and filter case history; - View case details, approvals, communication and participants information; - Remove case from archive	EHDS art. 68 (12), art. 87; Archiefwet
WP7-REQ-1.003	HDAB shall ensure processing of electronic health data such as the receiving, combining, preparing and compiling of necessary requested data from health data holders, the pseudonymisation or	Data Provisioning	Data is prepared, combined and pseudonymised/ anonymised by HDAB or the data holder before it becomes available to the data user in the SPE.	HDAB will provide a trusted data preparation environment, not accessible to data users, where requested data can be received from data holders and combined, prepared, and anonymized before it is made available in an SPE. - Data holder API for data delivery - Trusted data preparation environment	EHDS art. 57 par. 1(b)

	anonymisation of the data (EHDS article 57 par. 1 b).			accessible to HDAB case manager - Record linking - Pseudonymisation / anonymization according to the agreed standards - Delivery in SPE	
WP7-REQ-1.004	HDAB ensures that data are available for the data user within the SPE only for the time period stated in the data permit. (EHDS art. 68 par 10 sub e and par 12.)	SPE Management	Access to SPE is managed by permit information from DAAMs.	The SPE managed by HDAB as well as 3rd party SPEs must implement a state-of-the art IAA solution that: - Links user identity to data permits issued by the DAAMS process; - Allows the system to evaluate the time period for which the data permit is issued; - Allows the system to be alerted of any penalties or revoked permissions of the data user. The SPE managed by HDAB as well as 3rd party SPEs provide a mechanism for closing an SPE workspace or retracting data access after the data permit has expired or has been revoked.	EHDS art. 68 par 10 sub e and par 12.
WP7-REQ-2.001	Identifiable logs of access to and activities in the secure processing environment are maintained for the period necessary to verify and audit all processing activities in that environment. Access logs shall be kept for at least one year (Article 73 par 1 sub e).	SPE Management	Logging of: 1. access to the SPE by data users, 2. input and output to and from the SPE and 3. activities within the SPE. Retention of these logs for a minimum period not shorter than one year.	Logging of: 1. access to the SPE by data users, 2. input and output to and from the SPE and 3. activities within the SPE. Retention of these logs for a minimum period not shorter than one year.	EHDS 73 par 1 sub e

WP7-REQ-5.004	SPEs shall minimise the risk of the unauthorised reading, copying, modification or removal of electronic health data hosted in the SPEs through state-of-the-art technical and organisational measures. (EHDS art 73 par 1 sub b).	Privacy and Security	The SPE is designed with only authenticated access for persons and data as stated in the permit, and with controls on outgoing data. The risk of unauthorised access to or manipulation of the data is minimised.	The system will implement the following technical measures: - The SPE must encrypt data that are transferred to other project spaces within the SPE or to other SPE systems. The system will implement the following organizational measures. - HDAB provides proof of security by conducting periodic penetration tests and makes the results available to stakeholders.	EHDS art 73 par 1 b
WP7-REQ-5.005	Staff authorisation to enter SPE is based on access by necessity (EHDS art 73 par 1 sub c).	Privacy and Security	The SPE is set up with a management option with limited access for administrators. Record the reason for access.	HDAB must provide a staff authorization mechanism for data use and implement methods to validate the identities of administrative SPE users.	EHDS art 73 par 1 c
WP7-REQ-5.006	HDAB will only grant access to the SPE to the authorised natural persons listed in the respective data permit (EHDS article 73 par 1 sub a).	Privacy and Security	The SPE only grants access to the authorised natural persons listed in the respective data permit.	The SPE managed by HDAB as well as 3rd party SPEs must implement a state-of-the art IAA solution that allows for: - Identity validation; - Cross-border use; - Checking data user certifications; - Checking data permits, including their expiration date; Access to the SPE must only be granted to authorised individuals listed in the respective data permit, during the agreed time period and in absence of any penalties or revoked permissions linked to the data user.	EHDS art 73 par 1 a

WP7-REQ-5.007	HDAB must ensure that health data users have access only to the electronic health data covered by their data permit, by means of individual and unique user identities and confidential access modes (article 73 par 1 sub d).	Privacy and Security	In the SPE health data users only have access to the electronic health data covered by their data permit.	The SPE managed by HDAB as well as 3rd party SPEs must implement a state-of-the art IAA solution that allows for: - Identity validation; - Cross-border use; - Checking data user certifications; - Checking data permits, including their expiration date. Access to the SPEmust only be granted to authorized individuals listed in the respective data permit, during the agreed time period and in absence of any penalties or revoked permissions linked to the data user.	EHDS art 73 par 1 d
WP7-REQ-5.008	HDAB will ensure protection of privacy of the individuals or organisations captured within the data that is made available through the HDAB platform. (EHDS art 54)	Privacy and Security	Privacy protection is achieved through the use of encryption, access control and data pseudonymisation.	The system will provide technical data protection measures to ensure protection of privacy of the individuals or organisations captured within the data that is made available through the HDAB platform, including additional data protection/PET for datasets that contain personal data - or those datasets from which personal data can be derived by stacking them.	EHDS art 54
WP7-REQ-5.010	HDAB shall ensure by reviewing that the health data users are can only download non-personal electronic health data, including electronic health data in an anonymised statistical format	Output Control	Output data is checked for personal electronic health data.	The system must implement an export management system, including: - a process for data users to request export of any research output, including results, metadata, and analysis pipelines; - a staging area where output that is out for	EHDS art. 73 par. 2

	and output scripts from the secure processing environment. (article 73 par. 2).			review can be kept and shown to persons authorised for output control; - A process to review and accept or reject output requests on the basis of the absence or presence of personal data; - A mechanism that enables the data user to download approved output.	
WP7-REQ-5.014	HDAB ensures that data in the SPE is adequately pseudonymised or anonymised, in accordance with the data permit (EHDS art 66 par 3).	Privacy and Security	Data within the SPE must be sufficiently anonymised or pseudonymised.	The system implements a process to assess whether personal data are present in data sets uploaded by data holders, before these are made available in the SPE.	(EHDS art 66 par 3).
WP7-REQ-5.016	HDAB ensures that data from data holders can be uploaded in a secure way by the data holders to the SPE (EHDS art. 73 par. 2).	Data Provisioning	The SPE provides secure data import from data holder or trusted data exchange solution.	The system must implement a solution that enables: - Data holders to securely upload data to the SPE for use by the data user - Data holders to give the SPE secure access to an SPE holding the requested data set for federated analysis - HDAB give the SPE access to data combined or prepared in the internal SPE for processing by the data user	EHDS art. 73 par. 2
WP7-REQ-5.017	HDAB will ensure emergency protocols are available for a general lockdown of the HDAB platform and SPE in case of security issues, data leaks or other high impact incidents or risks. Initiating a lock down can	Privacy and Security	The SPE management plan includes a disaster preparedness plan, in which the SPE environment can be made completely inaccessible in the event of a serious incident.	Set up a disaster preparedness plan. Create a technical possibility to (temporarily) completely shut down an SPE.	

	be requested by security officers in which case the SPE operators execute the workspace(s) (temporary) lock down.				
WP7-REQ-5.019	HDAB shall provide a mechanism for data holders to upload data to the SPE in the format determined by the data permit (article 73 par. 2).	Data Provisioning	The SPE provides data import, allowing all requested/agreed data formats.	The system must implement a solution that enables: - Data holders to securely upload data to the SPE for use by the data user - Data holders to give the SPE secure access to an SPE holding the requested data set for federated analysis - HDAB give the SPE access to data combined or prepared in the internal SPE for processing by the data user The solution must be data format agnostic.	EHDS art. 73 par. 2
WP7-REQ-5.020	HDAB shall ensure regular audits, including by third parties, of the secure processing environments and shall take corrective action for any shortcomings, risks or vulnerabilities identified by those audits in the secure processing environments (article 73 par. 3).	SPE Management	The system supports regular audits, including external audits, to ensure compliance with operational and security requirements.	The system must support regular audits, including external audits, to ensure compliance with operational and security requirements.	EHDS 73 par 3
WP7-REQ-5.021	HDAB shall ensure that the SPE managed by HDAB as well as 3rd party SPEs that are certified and approved to be operated within	SPE Management	HDAB ensures that all SPEs within HDAB meet legal, technical and operational requirements for certification.	HDAB shall implement certification procedures to ensure that the SPE managed by HDAB as well as 3rd party SPEs that are certified and approved to be operated	EHDS art 73 E, art. 57 par. 1 sub a under i

	the HDAB environment will conform to all statutory regulations. (EHDS art 73 E, art. 57 par. 1 sub a under i)			within the HDAB environment will conform to all statutory regulations.	
WP7-REQ-6.005	HDAB shall ensure compliance with and monitoring of the security measures referred to in EHDS art 73 par 1 to mitigate potential security threats. (EHDS art 73 par. 1 sub f)	Privacy and Security	The safety measures surrounding the SPE are monitored.	HDAB shall implement logging and internal auditing procedures, including regular penetration tests, to monitor the security measures referred to in art 73to mitigate potential security threats.	EHDS art 73 par 1 sub f
WP7-REQ-6.008	HDAB shall ensure the SPE managed by HDAB as well as 3rd party SPEs are GDPR compliant. (EHDS art 77 (consideration), EHDS art 74)	Privacy and Security	Controlling and ensuring data access and data transfers are GDPR compliant.	HDAB shall implement auditing and certification procedures to ensure that the SPE managed by HDAB as well as 3rd party SPEs are GDPR compliant.	EHDS art 77 (consideration), EHDS art 74
WP7-REQ-6.010	HDAB implements requirements following from implementation acts adopted by the European Commission, specifying technical, organisational, information security, confidentiality, data protection and interoperability requirements for the secure processing environments, including the technical features and tools available to the user of health data in the secure processing environment. (EHDS	SPE Management	Processes regarding requirements following the implementation acts.	Requirements following from the implementation acts regarding the SPE.	EHDS art. 73 , art. 55 en 57 par 1 under g

	art. 73 par 5, art. 55 and 57 par 1 under g)				
WP7-REQ-4.7	HDAB must ensure that the security and infrastructure of the SPE is audited based on European standards supplemented with national standards. HDAB must provide HDAB managed Secure Processing Environments (SPEs). HDAB must provide a certification track for 3rd party managed secure processing environments (SPE). (EHDS art 73 par 3)	Privacy and Security	HDAB ensures robust security and compliance by auditing the SPE infrastructure against European and national standards. HDAB provides secure environments for data processing while enabling third-party SPEs to be HDAB-certified.	The system must support regular security and infrastructure audits of SPEs based on European and supplementary national standards. Provide a standardised HDAB-managed SPE with predefined security, privacy, and compliance configurations. Develop a certification track for third-party SPEs, including guidelines, evaluation criteria, and compliance checks.	EHDS art. 73(3)

Health
Data Access
Body-NL

Denk mee. Praat mee. Bouw mee.

Health
Data Access
Body-NL

Denk mee. Praat mee. Bouw mee.