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: D5.1: DAAMs: Requirements, Specifications and Prototype.

Starting date of the project: December 1st 2023.

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

Work package (task): WP5 Data Access Applications Management solution (DAAMs – T. 5.1)

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 (HDAB) in the Netherlands together with its supporting digital business capabilities over a four-year period.

Work package 5 (WP 5) aims to enable the Netherlands' HDAB to receive, process and respond to data access applications and to issue/manage data permits. The first steps for a successful implementation of the Data Access Applications Management solution (DAAMs) entails "Analysis and design" activities. While these activities during the first phase of the project officially terminate with this Deliverable 5.1 (D5.1), they will need to be revisited when the recommendations from the Joint Action Towards the European Health Data Space (TEHDAS2) on secondary use become available, as well as more lessons learnt from the HealthData@EU pilot.

Several milestones (MS) were developed as building blocks towards this Deliverable 5.1 (D5.1); the completion of the analysis and design (T5.1) phase.

- MS 5.1.1: an overview was made of existing DAAMs solutions and components that could form part of the DAAMs of HDAB-NL.
- MS 5.1.2: an analysis of the legal requirements imposed by the European Health Data Space regulation (EHDS) on the DAAMs, along with an assessment of the extent to which existing solutions meet the preconditions that the EHDS aims for.
- MS 5.1.3: stakeholder analyses. To ensure that the Deliverable 5.1 represents a new DAAMs design that makes optimal use of current DAAMs-like solutions, national stakeholders have been included as early as possible in the process to consult on business and stakeholder requirements. European stakeholders are those consulted in the EHDS2 Community of Practice (subgroup 1) and the HealthData@EU pilot.

Based on the first milestones and further legal and functional analyses, functional components have been identified that together should cover the entire DAAMS functionality. A division has been made between core components that describe the primary processes of the DAAMS portal and supporting components that must fulfil the non-functional requirements of the DAAMS portal; see Figure 4 in Chapter 8. Based on the legal requirements and the mapping of functional requirements a first inventory (high abstraction) of functional blocks was described. With the completion of phase 1, in 2025 and 2026, phase 2 will focus on completing this list with business and stakeholder requirements. This also means revisiting this deliverable and aligning (where necessary) with output from TEHDAS2 and HealthData@EU results. 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 WP5 team will keep involving out stakeholder community to ensure our solution is consistent with their needs and makes a positive impact on the user and data holder requirements in the Dutch Health Data landscape.

2. Abbreviations

Abbreviation	Description
Art	Article
CPU	Central Processing Unit
DAAMs	Data Access Applications Management solution
DPO	Data Protection Officer
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
SPE	Secure Processing Environment
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 (further mentioned as '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 (further mentioned as 'applicant'):*
  A natural or legal person submitting a health data access application for a permit as described in article 68 EHDS.
- *Health data request (further mentioned as 'request'):*
  A request as described in article 69 EHDS.
- *Health data requestor (further mentioned as 'requestor'):*
  A natural or legal person submitting a request as described in article 69 EHDS.

Table of Contents

4. Introduction to work package 5: the Data Access Applications Management solution (DAAMs)

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 (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.

Work package 5 (WP 5) aims to enable the Netherlands' coordinating health data access body to receive, process and respond to data access applications and to issue/manage data permits:

- Define requirements and specifications for the Data Access Applications Management solution (DAAMs);
- Design an architecture for the DAAMs based on reusing existing components where feasible;
- Implement and pilot the DAAMs using real-world use cases;
- Launch an operational DAAMs accessible for the entire Dutch health data community.

5. Description of the First Deliverable

T5.1 Data Access Applications Management solution (DAAMs): Analysis and Design – as described in the Grant Agreement

The first steps for a successful implementation of the Data Access Applications Management solution (DAAMs) entail "Analysis and design" activities. While these activities during the first phase of the project officially terminate with this Deliverable 5.1 (D5.1), 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 from the HealthData@EU pilot. This is necessary to ensure alignment and interoperability with the other European health data access bodies' DAAMs. Nonetheless, we expect the results in this D5.1 to not deviate significantly from what TEHDAS2 and the HealthData@EU pilot will deliver, and thereby an important first steppingstone towards a future final list of requirements and specifications for the DAAMs of HDAB-NL.

The solution design for WP5 has many interactions and dependencies with other work-packages. The design process will be iterative and closely aligned with the design process for the other work-package such as (WP6 (catalogue), WP7 (Secure Processing Environment for Health Data) and WP8 (Infrastructural solutions (cross-border gateway & generic services) since the DAAMs needs to integrate with all of them. Requirements and specifications are set to be demonstrated in 2026 with the use of a prototype supporting stakeholders to accurately understand and scrutinise the requirements and specifications for the DAAMs.

6. Approach

Work plan for WP5 – zooming in on the milestones part of T5.1

Several milestones (MS) were developed as building blocks towards this Deliverable 5.1 (D5.1); the completion of the analysis and design (T5.1) phase.

- MS 5.1.1: an overview was made of existing DAAMs solutions and components that could form part of the DAAMs of HDAB-NL. This was done by investigation of the Dutch landscape but also taking some advanced access portals of other European member states as examples. Several visualisations and flow diagrams to map out the entire data request process (reception, processing, responding, executing) for different types of health data were also developed – see next chapter).

  Specifically for this milestone, the WP5 team:

  - 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 (sub group 1) to learn from similar DAAMs efforts in other European member states;

- MS 5.1.2: an analysis of the legal requirements imposed by the EHDS on the DAAMs, along with an assessment of the extent to which existing solutions meet the preconditions that the EHDS aims for. It should be taken into account that the EHDS framework is quite abstract; the new Joint Action Towards a European Health Data Space (TEHDAS2) will come up with recommendations for implementation acts, which need to be harmonised with the HDAB-NL. In addition, the objection procedure will be a side process in the DAAMs that needs to be further developed in subsequent phases. Legal requirements as described in this document will still need to be carefully reviewed by legal experts now the EHDS has almost been finalised (EHDS version November 27, 2024).

  Specifically for this milestone:
  - Learned from our partners working on WP10 about the legal requirements of the EHDS, implications for the DAAMs, the HDAB-NL governance structure, and technical business capabilities which link the technical work packages.

- MS 5.1.3: stakeholder analyses. To ensure that the final Deliverable 5.1 represents a new DAAMs design that makes optimal use of current DAAMs-like solutions, national stakeholders have been included as early as possible in the process to consult on business and stakeholder requirements. European stakeholders are those consulted in the EHDS2 Community of Practice (subgroup 1) and the HealthData@EU pilot.

  Specifically for this milestone:
  - We organised an explorative first session to investigate current user journeys for data holders, researchers, policy makers, IT specialists and other groups, in June 2024;
  - We organised two DAAMs break-out sessions as part of the HDAB-NL kick-off in September 2024 to receive further input for requirements and specifications;
  - 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 to be included in the next phase of requirements and specifications;
  - We processed this feedback and comments into the currently presented legal requirements overview and have materials ready to be reviewed and integrated in subsequent phases when we integrate the business and stakeholder requirements.

Delays and versioning of requirements

Unfortunately, we have had a slow start due to the delay of the final EHDS publication.

We expect that after delivery of D5.1 in March 2025, we will need to revisit the requirements based on the final publication of the EHDS for potential adjustments. **Therefore, it must be noted that the**

legal requirements presented in this report cannot be regarded as final (though significant deviations when compared with the final EHDS text are not expected). And again, this text only presents legal requirements. Business and stakeholder requirements will be included in the next phase.

Updated versions are to be expected throughout the project, and also when national legislation is put into place related to the national implementation of the EHDS. As mentioned, the new Joint Action Towards a European Health Data Space (TEHDAS2) will come up with recommendations for implementation acts, which also need to be harmonised with the HDAB-NL and DAAMs 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, D5.1 will therefore remain an iterative work in progress.

7. Outcomes preliminary studies

Milestone 5.1.1: an overview of existing DAAMs solutions

In Q1 2024, examples of existing (inter)national examples of DAAMs-like systems were researched. Subsequently, based on the core components identified in milestone 5.1.2, an inventory was made of core components present in each instance.

Information was gathered from a total of eight DAAMs-like systems. Annex 1 briefly describes to what extent each system has incorporated the main elements as identified in the EHDS for the DAAMs (see milestone 5.1.2).

It is important to note that the core components presented in this section constituted a baseline analysis to start our work for work package 5 and was based on a previous version of the EHDS (March 2024). Eventually with more elaborate legal analyses, architecture studies related to work package 8, stakeholder information, and a later version of the EHDS text (Nov 27, 2024), we developed a more complete component model which will form the basis of the requirements and specifications for the DAAMs. This can be found in the next chapter. In other words, MS 5.1.1. and MS 5.1.2. represent stepping stones towards the final D5.1.

Finally, several visualisations and flow diagrams to map out the entire data request process (reception, processing, responding, executing) for different types of health data were also developed.

Milestone 5.1.2: EHDS legal requirements for the DAAMs

The concept version (March, 2024) of the EHDS legal text provided a first framework for the functionalities of the DAAMs and the HDAB-NL. In order to gain insight into these functionalities, or business capabilities, and legal requirements for the DAAMs, a high-over overview of the main elements related to the DAAMs was developed. This was a first rough inventory based on the concept EHDS text; a stepping stone to a more complete and up to date component model that will follow later in this document.

This first analysis of MS 5.1.2 yielded a number of functionalities that are related and complementary to each other. Subsequently these functionalities were grouped using a method based on two sources:

- an analysis by Health-RI, carried out for the purpose of procurement of a data request tool. In short, results showed that a DAAMs contains three core components: request form, request portal, request registry services;
- a report from the Health Data Agency (HDA), the Belgian HDAB. This resulted in four core components: submission process, identification of data suppliers, processing and validating requests, and follow-up and handling of requests.

Our very first high-over analysis eventually grouped the DAAMs functionalities into four core components: requesting, processing, informing, and registration. This grouping is shown in Appendix 1. Some functionalities contribute to multiple core components and are therefore mentioned more than once. Appendix 2 shows the EHDS requirements for DAAMs and implications in more detail.

The text of the EHDS (November 27, 2024), presents a list of regulations and legal requirements for the HDAB that touch directly or indirectly (by cross-referencing or demarcating the functional limits of the DAAMs) on the desired functionalities of the DAAMs.

The relevant articles and paragraphs will be listed here with their relevance for the DAAMs briefly outlined. After, the mentioned articles with the relevant paragraphs are listed in full. Subsequently, in Chapter 8, this information directly taken from the EHDS text (version Nov 27, 2024), along with MS5.1.2, will provide the base for the component model. There, the legal requirements are colocated along with their business processes among the functional core and supporting components.

The following articles from the EHDS (November 27, 2024) are highlighted here because they relate to the functionality of the DAAMs and because they cross-reference each other when setting criteria for health data applications and requests. Appendix 1 includes all mentioned articles in full.

- Article 2 Definitions relevant for the HDAB and DAAMs;
- Article 51: defines which data categories apply for applications and requests to be processed in the HDAB/DAAMs;
- Article 53 & 54: define which purposes are permitted and prohibited for processing secondary health data requests and applications under the EHDS and within the DAAMs;
- Article 55, 57, 58: defines the roles, tasks, and obligations of the HDAB, where the DAAMs is relevant;
- Article 59: lists the reporting duties of the HDAB, where the DAAMs will serve as a source of information;

- Article 60: lists the duties of data holders participating within the HDAB and DAAMs systems;
- Article 61: lists the duties of health data users within the HDAB/DAAMs system;
- Article 62: lists regulations around cost-setting and fees for the HDAB/DAAMs;
- Article 66: discusses data minimisation and purpose limitation, which function as criteria when assessing health data requests and applications;
- Article 67: lists regulations related to health data access applications to be received and processed by the DAAMs;
- Article 68: lists regulations related to data permits provided by the DAAMs;
- Article 69: lists regulations related to health data requests to be received and processed by the DAAMs;
- Article 70: provides information regarding future templates to support access to electronic health data for secondary use;
- Article 71: defines regulations regarding the right to opt out from the processing of personal electronic health data for secondary use;
- Article 72: defines the simplified procedure for access to electronic health data from a trusted health data holder;
- Article 73: stipulates regulations regarding the request and provision of a Secure Processing Environment (SPE) through the DAAMs.
- Article 81: stipulates the right and procedure to lodge a complaint with a health data access body.

Milestone 5.1.3: national and international stakeholder engagement

National stakeholder engagement

In June of 2024, we organised a stakeholder meeting to 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 working reality of these stakeholder groups in the Dutch fragmented health data landscape.

During two break-out sessions of the official national HDAB-NL kick-off in September 2024, we asked about business and stakeholder requirements for the future HDAB-NL and DAAMs. For this interactive session we had identified eight thematic components within the user journey, so we could ask input on desired functionalities within each component during the session. 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 concept version of the EHDS, stakeholder sessions, and several DAAMs-like systems as identified in MS 5.1.1. This only represented one third of the requirements; the business and stakeholder requirements were not yet included. For these we had identified a list based on the same sources and asked them to participate in a prioritisation exercise. We are currently waiting for their input and are keen to again incorporate this into a first draft of the business and stakeholder requirements in Q1 and Q2 of 2025.

Collaboration within EHDS2 CoP SG3 and HealthData@EU

We have joined the EHDS2 CoP Subgroup 1 on the DAAMs. Every two 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 regarding the DAAMs. In this CoP Subgroup we also keep track of HealthData@EU developments.

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 recommendations for implementing acts coming out of TEHDAS2.

8. Component model

As a first step in exploring the width of HDAB functionality, in the context of work package 5 (DAAMS) roles and basic interactions were identified, and their position in and around DAAMS was depicted (figure 1).

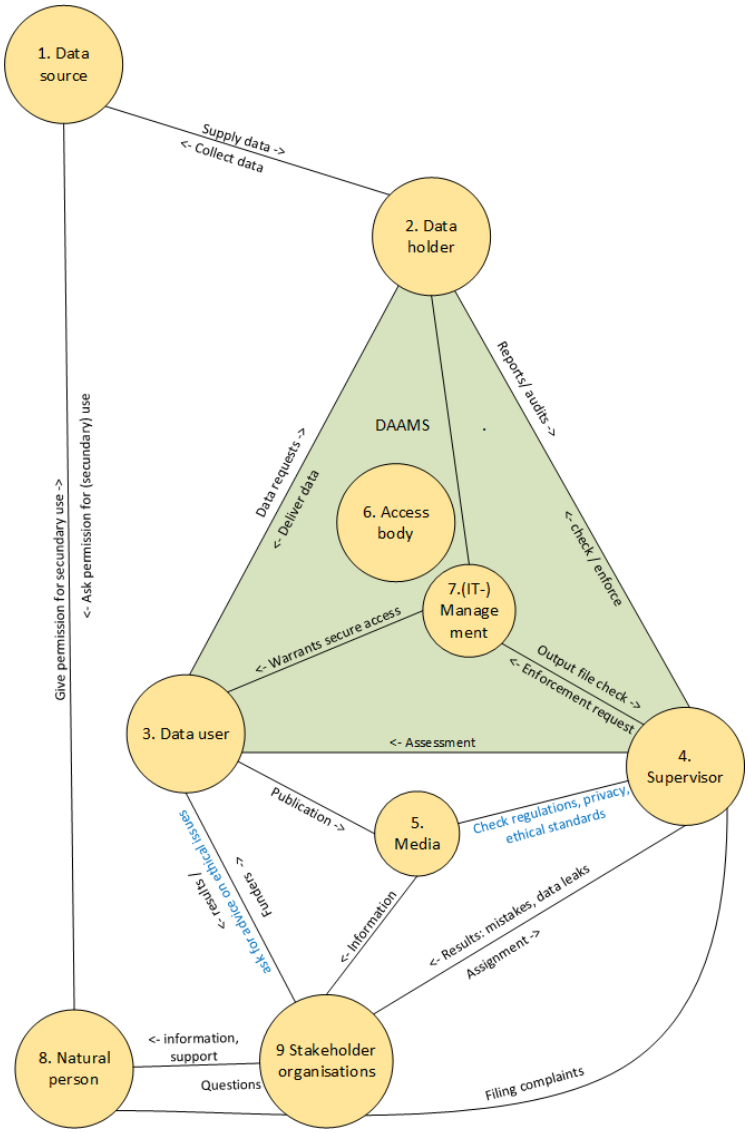

Figure 1: Roles around DAAMs

Secondly (figure 2 and 3) more of the interactions between the main players around DAAMS, being the data holder, the –aspirant- data user and HDAB itself are identified. Through these interactions the necessity of different services becomes clear: application service, access control, output control, encryption service, et cetera.

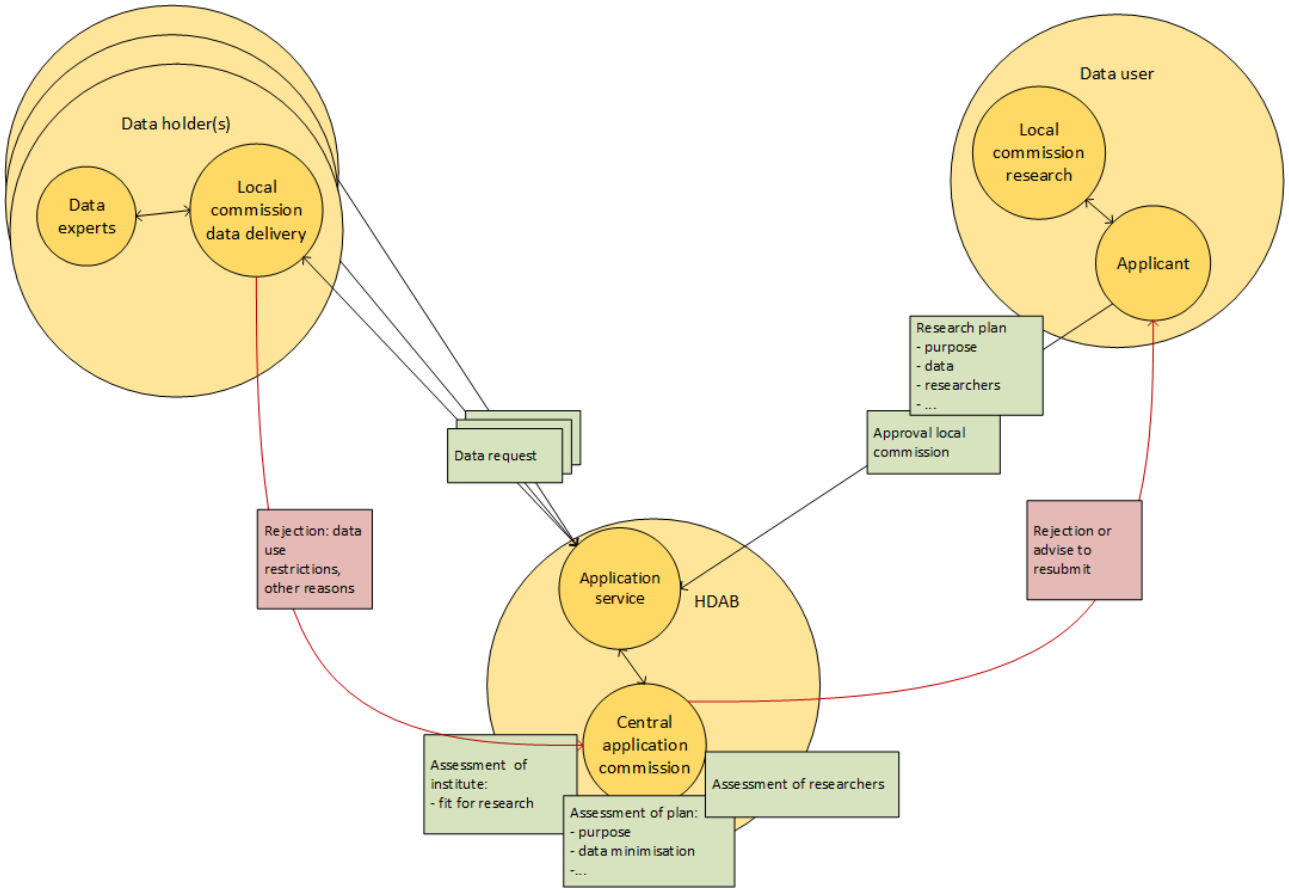

Figure 2: Application actions through HDAB (DAAMs)

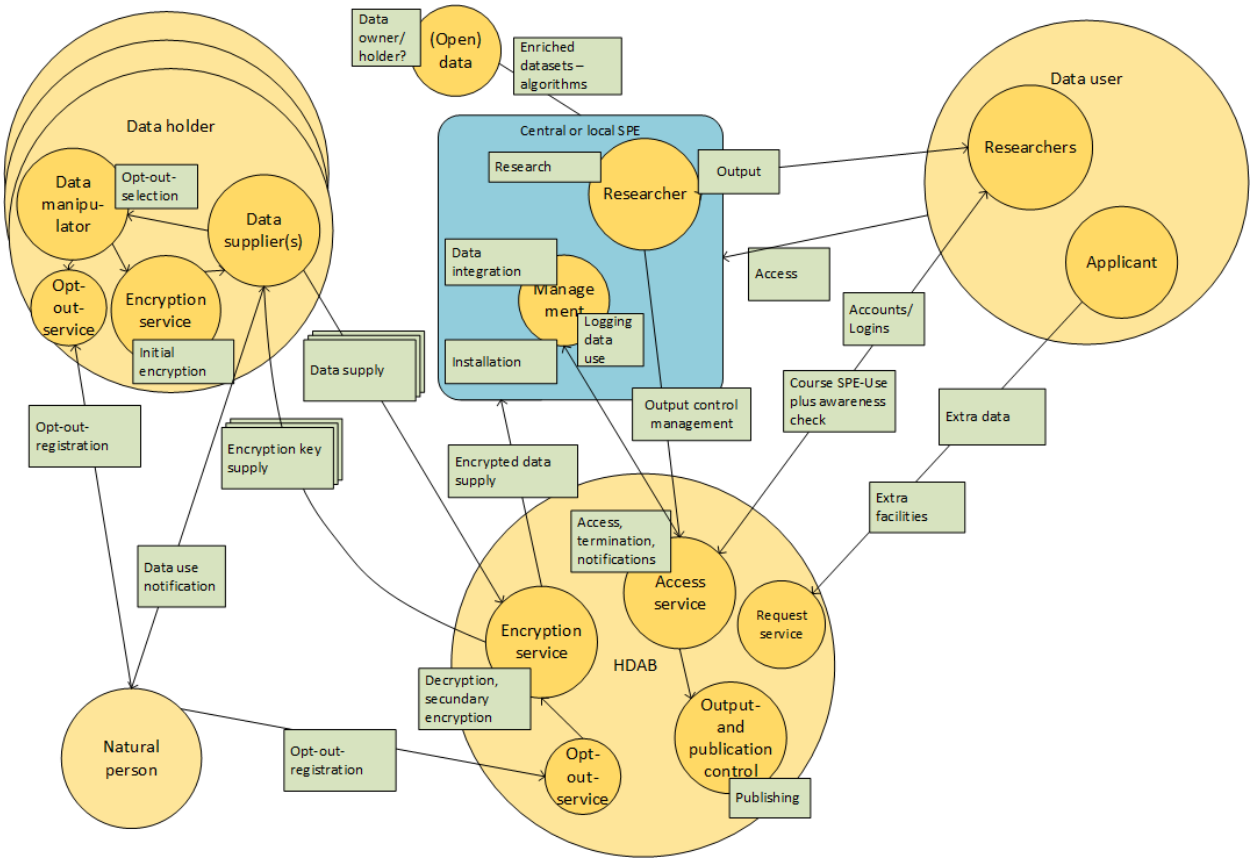

Figure 3: HDAB organisation units with data delivery in use

These initial analyses were corroborated by the HDAB blueprint (in concept) presented at the Cross CoP SG meeting in December 2024. The further development of this blueprint will be taken into account in the next steps of WP5 in 2025.

Based on these insights and using the first milestones (MS5.1.1 and MS 5.1.2) a component model (figure 4) has been structured, containing functional components that together should cover the entire DAAMS functionality. A division has been made between core components that describe the primary processes of the DAAMS portal and supporting components that must fulfil the non-functional requirements of the DAAMS portal.

In this component model, the components displayed below in grey have a relation to the DAAMS core components but are not covered in this document.

***Note**: 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.*

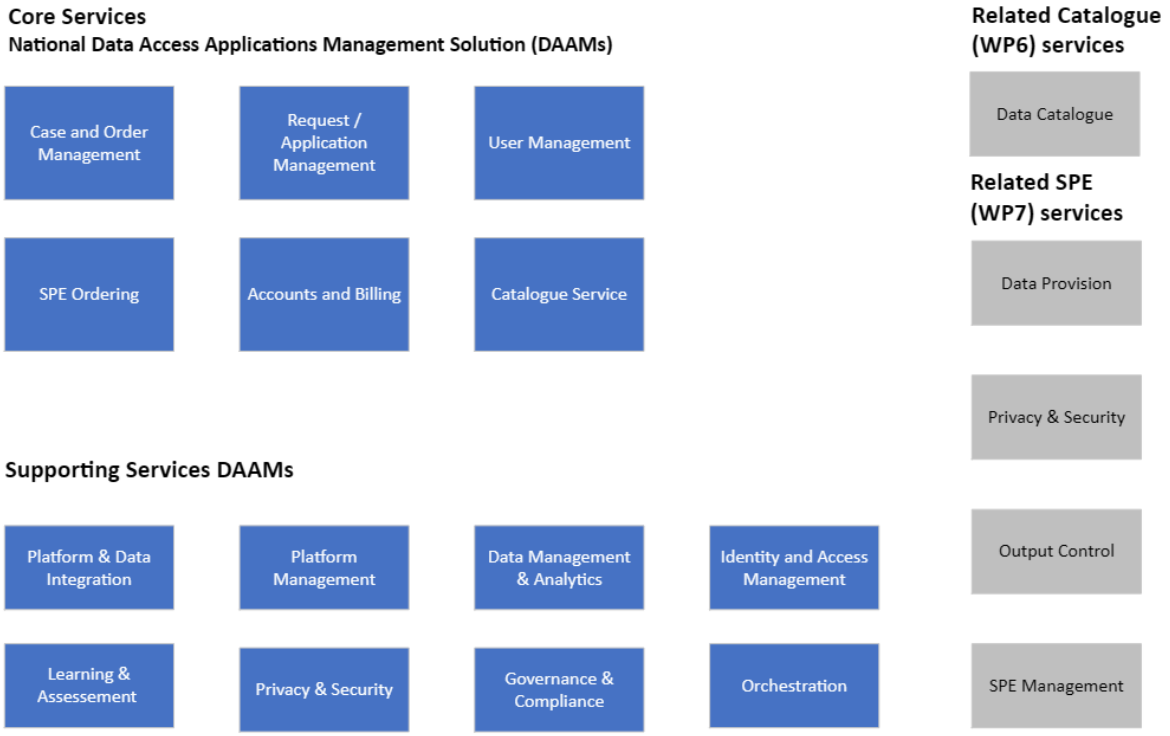

Figure 4 – Component model of DAAMs services

First, each **core component** will be described below, after which its legal requirements (with the related EHDS Articles) are identified and business processes described (see Appendix 1 for all relevant EHDS articles and Appendix 4 for an overview of the legal requirements).

Case and Order Management

A Case and Order Management system is a platform or software solution that allows managers of the HDAB platform to track requests, process request orders, assign workflows and streamline process completion. Its goal is to ensure that the correct data products end up in the hands of the data users who requested them. It ensures that data/information requests are delivered as expected according to the details stipulated on the request form and as stated in the permit, with full order transparency and timely completion of the request.

Therefore, the legal requirements mentioned below are related to many of the EHDS Articles (EHDS, text version Nov 27, 2024) listed in MS 5.1.2, including (but not limited to): Articles 55, 57, 58, 60, 61, 67, 68, 69, 71, 72, 73, and 81.

The goal of a Case and Order Management system is to streamline the entire process from beginning to end. By automating many of the tasks involved in managing orders, HDAB data users and data holders can save time and money while administrators ensure accuracy and efficiency.

This system supports the following core processes:

- Receipt of requests and applications;
- Automations and workflow management;
- Request and application processing;
- Feedback and request for additional information from data user.

The following legal requirements are part of this component (see Appendix 4 for a copy with all legal requirements and the article numbers according to the December 2024 version of the EHDS):

- **Requirement 1.1[1]:** HDAB must assess a data request or health data access application and give permission based on the information provided by the requestor/ applicant and the assessment criteria from the EHDS that a request or application must meet (EHDS art. 57 (1)(a), art. 67 and 68).

  Business process of this requirement: Completed request/application forms must be distributed to an assessment body (within or by HDAB), the request/application must be assessed, and assessment, results must be returned to the requestor/applicant.

- **Requirement 2.10:** HDAB must check whether HDAB permitted research has been published within the period stated following the EHDS (EHDS art. 57 (1)(a)(iv), art. 61(4) EHDS).

  Business process of this requirement: For each research project permitted by HDAB a preliminary title and description of one or more publications must be added within the statutory period, plus the estimated time of publication, also within the statutorily demanded period. Users are obliged to add the actual publication plus link to their research dossier in the HDAB portal and HDAB must flag when no actual publications are registered within the demanded period.

- **Requirement 2.17:** HDAB must provide a management system for registering and processing applications and requests and decisions regarding the received requests/applications (EHDS art 57 (1) (e) and (j)).

  Business process of this requirement: Management of the registration and processing of applications and requests, as well as the decisions regarding the received requests/applications, including noting responsibilities of different participants in the various stages of the process.

- **Requirement 2.21:** HDAB must upon receiving an application verify that the applicant satisfies the demands with regard to technical and organisational measures for prevention of misuse (EHDS art 68(1) (d) and (e)).

  Business process for this requirement: HDAB checks if applicants meet EHDS requirements to work with the data applied for.

[1] The numbering of these requirements is based on a more complete inventory including not only legal requirements but also business and stakeholder requirements. The list with only legal requirements is in Appendix 4

- **Requirement 2.22:** HDAB must, upon receiving an application, verify the identity, authorisation of the applicant as well as their qualifications regarding the use of the requested data and the research that is to be done with that data (EHDS art. 67(2)(a), art. 68(1)(d)).

  Business process for this requirement: Upon receipt of application HDAB follows an assessment procedure starting with identification of the applicant.

- **Requirement 2.26:** HDAB is able to forward data requests to a data holder.

  Business process for this requirement: After issuing a permit to researchers by HDAB their data requests must be transmitted to data holders (EHDS art. 72(3).

- **Requirement 2.27:** HDAB shall issue or refuse a data permit within 3 months of receiving a complete data access application, with an extension maximum of three months taking into account the urgency and complexity of the request and the volume of requests submitted for decision (EHDS art. 68(4).

  Business process for this requirement: HDAB processes applications and ensures that decisions are made within the mandated 3-month timeframe after receiving the application or informs the applicant of any delay.

  Requirement 2.29: HDAB must, in case of a complaint, provide information on the receipt, processing and resolution of the complaint (EHDS art. 81 (1) and (3)).

  Business process for this requirement: HDAB installs a logging and publishing system for all phases and types of complaints.

Request / Application Management

Request / Application Management is closely linked to Case and Order Management but deals with the actions of the applicant or requestor. Request/application completion is user-friendly, with decisions made visible to the customer throughout the process. It provides the data requestor with up-to-date information on existing requests, allows the submission of new requests and/or saves draft requests. For each submission the data requestor is able to see the allocated workflow, the status of each step in the flow and corresponding permits organised by project. Applications can be completed in Dutch or English. Previous permit and organisational data from the data requestor are automatically filled in to ease form completion.

The legal requirements outlined below are related to many of the EHDS Articles (version Nov 27, 2024) listed in MS 5.1.2; including (but not limited to): Articles 53, 54, 57, 58, 61, 66, 67, 68, 69, 70, 72 and 73.

This system supports the following core processes:

- Request / application creation: Facilitates the process of creating and submitting new data requests or applications in a structured and user-friendly manner;

- Request / application assessments: Involves evaluating the submitted requests or applications for completeness, validity, and adherence to the specified requirements;
- Dataset selection;
- Management of request / application attachments;
- Request / application management (e.g., modify, submit, delete, check-status);
- Request / application verification (assess whether all information has been provided);
- Request / application history and research results reference.

The following legal requirements are part of this component:

- **Requirement 2.7:** HDAB must provide the possibility to apply for two types of requests/applications: information requests (EHDS art. 69(2)) and applications for data research (EHDS art 68(2)).

  Business process for this requirement: HDAB provides predefined digital forms for both data requests and health data access applications.

- **Requirement 2.3:** The researcher applying for data access must provide an estimation of the period during which the electronic health data is needed for processing.

  Business process for this requirement: HDAB provides applicants with a process to provide information about the period of time which they need to process (= do research on) the requested data (EHDS art. 67 par. 2 sub h).

- **Requirement 2.4:** HDAB must register, as part of the registered health data access applications, a description of the expected results of each research request available (EHDS art. 57 par 1 sub j and art 58 par 1).

  Business process for this requirement: HDAB provides a procedure to provide information about expected results of the research from each application.

- **Requirement 2.5:** HDAB must provide functionality through which the user of the platform is able to see the status of a submitted data request or application (EHDS art 57 (1) (e)).

  Business process for this requirement: HDAB provides functionality through which the user of the platform is able to see the status of a submitted data request or application.

- **Requirement 2.8:** HDAB must provide functionality for an accelerated application procedure for specific bodies and reasons (EHDS 68(6)). In that case a decision takes place within two months of receipt, with an extension maximum of one month (EHDS art. 68(6)).

  Business process for this requirement: HDAB recognises and processes urgent data requests as such when appropriately flagged.

- **Requirement 2.41:** HDAB must provide a process to request research results (health data request). HDAB shall assess the data request within 3 months. HDAB shall also provide the result of the data request to the requestor within 3 months (EHDS 69.1).

Business process for this requirement: HDAB provides a process to request research results. HDAB assesses the request within 3 months. HDAB also provides and publishes the result of the request within 3 months.

- **Requirement 4.19:** HDAB must (be allowed to) take decisions on applications with purposes for secondary use as defined by the EHDS, within 3 months of receipt, up to 3-month extension possible (EHDS 68.4, 68.6).

  Business process for this requirement: HDAB processes applications and ensures that decisions are made within the mandated 3-month timeframe, with a possible 3-month extension under justified circumstances.

- **Requirement 4.22:** HDAB must facilitate research on data from other (EER) countries when a request for this data is incorporated in a licensed application (EHDS 75).

  Business process for this requirement: The HDAB enables cross-border research by incorporating data requests from other EER countries into licensed applications. Other data (from EER countries) than only catalogue data can be added to a research request.

- **Requirement 5.2:** The HDAB system needs to, as part of the application process, facilitate functionality where the applicant describes the limited purpose of the data that is requested (EHDS 67(2) b-d).

  Business process for this requirement: Within the DAAMs system, the applicant must be able to indicate the reasons for the requested data (purpose of the research/basis).

User Management

The DAAMS system serves multiple user roles, including data users (requestors and applicants), data holders, and other roles such as administrators and output controllers. All users must register with HDAB-NL. In cases where multiple HDAB bodies are involved, there must be a single central repository or a referring system that consolidates information on system participants, data users, and data holders. The core functionality supporting this component is Customer Relationship Management (CRM).

A CRM system serves as a hub for organising information on users, providing the input and tools needed to collect and manage information about people and organisations that work within the HDAB environment. It allows for the collection of user information, including contact information, credentials, connectivity, permits and communication preferences regarding request processing, requests for and SPE fulfilment.

This system supports the following core processes:

- Register roles e.g. researchers, institutes, public organisations, and others;
- Self-service registration;
- Maintain and manage customer data;
- Manage customer permits;
- Manage customer attestation;
- Manage customer communication.

The following legal requirements are part of this component:

The EHDS does not stipulate any legal requirements for this component.

SPE Ordering

SPE Ordering is a component that only concerns applicants for a HDAB research permit. The various types of safe research environments for applicants are dealt with in WP7.

The HDAB service portal enables the ordering of a Secure Processing Environment (SPE) for projects with a research permit issued by HDAB. The individuals specified in the order are verified against those listed in the permit. If project information is available in the service, orders are linked to the corresponding project. The legal requirements belonging to this core component are related to the following EHDS Articles (version Nov 27, 2024) listed in MS 5.1.2 (though not limited to): Articles 51, 55, 60, 61, 66, 67, 68, 69, and 73.

The portal provides an easy way to order a SPE following a predefined process and provides the ability to customise the availability of specific tools and other characteristics within the SPE environment.

This system supports the following core processes:

- SPE ordering;
- Receipt of approved applications;
- Receipt of SPE order;
- Fulfilment of SPE order.

The following legal requirements are part of this component:

- **Requirement 2.24:** HDAB must make requested datasets available to researchers in a SPE within 60 days after receiving the data (EHDS 68(7)).

  Business process: HDAB keeps track of date of reception of the data from data holder and date of providing the data to the data user in a SPE.

- **Requirement 4.16:** HDAB must ensure that data usage agreements include provisions regarding the time limitations for data usage and storage. These agreements are shared with the data applicant or requestor during the ordering process (EHDS 68, 69).

  Business process for this requirement: HDAB manages usage agreements with regard to time limitations for data usage and storage. These agreements are shared with the applicant during the ordering process, and compliance is monitored throughout the provision phase.

- **Requirement 5.1:** HDAB must provide an overview of the system requirements and security prerequisites that allow the configuration of a SPE and provision of access to verified users (EHDS art 55).

  Business process for this requirement: In DAAMs, the requirements and wishes of the data user for a SPE may be specified, within the boundaries of the EHDS requirements, and the access rights for the user may be regulated.

- **Requirement 7.6:** HDAB must provide a Secure Processing Environment (SPE) in which the researcher can execute his/her research on the requested datasets (EHDS art 73).

  Business process for this requirement: The provision of a SPE by HDAB.

Accounts and Billing

HDAB-NL uses the DAAMS system to manage permits, issued datasets, and the use of Secure Processing Environments (SPEs). Within the HDAB ecosystem, DAAMS also serves as a clearing house in its central role, especially when costs are associated with accessing requested datasets.

The clearing house by HDAB acts as a third-party mediator between the data user (buyer), the data holder (seller), and the SPE host, involved in a financial transaction. Fees charged to data users are distributed to cover the costs incurred by data holders for making data available. The clearing house's primary responsibilities include ensuring that transactions comply with applicable rules and regulations and that payments are accurately credited to the correct beneficiary.

The legal requirements outlined below are related to many of the EHDS Articles (version Nov 27, 2024l listed in MS 5.1.2; including (but not limited to): Articles 55, 57, 58, 59, 62, 67, 68, 69, and 73.

This system supports the following core processes:

- Scrubbing of payment claims;
- The clearing house is responsible for matching the seller and buyer transactions. This means that it is the responsibility of the clearing house to set up a process that ensures payments are always credited to the correct beneficiary without fail;
- Clearing houses consolidate all transactions between data users and data holders in the HDAB system. Instead of asking for several small payments, clearing houses consolidate and provide the HDAB data users and data holders with one statement. The details of the debits and credits are listed as line items on that statement. This simplifies the record-keeping process and the process for the HDAB data users and data holders;
- Clearing houses also perform other tasks such as collection and dissemination of information, which helps in conducting analyses of the payment transactions;
- Reporting on financial/payment transactions.

The following legal requirements are part of this component:

- **Requirement 2.23:** HDAB may charge a different fee per data user where this is demanded by national guidelines (EHDS art 62).

  Business process for this requirement: The HDAB determines a fee for each request or application, based on national guidelines.

- **Requirement 4.11:** HDAB must calculate fees according to national and/or European policies (EHDS art 62).

  Business process for this requirement: Fees are calculated in line with the national and/or EU policy principles.

- **Requirement 4.12:** HDAB may charge a fee that is in proportion to the cost of making available electronic health data for secondary use, including the evaluation and processing of data access requests (EHDS art 62).

  Business process for this requirement: Fees for EHDS compliance are calculated and published, covering both the costs of data provisioning and the assessment of requests.

- **Requirement 5.4:** Any fees charged to health data users by the health data access bodies or health data holders (EHDS art. 62) shall be transparent and non-discriminatory (EHDS art 62(3)).

  Business process for this requirement: Organising payments to data users and compensation to data holders. Data usage fees are transparent during the application process.

Catalogue Service

Through the DAAMS portal, users can access the Health Data Catalogue (HDC) service, which allows them to select, filter, and link the datasets needed for research. The functionality of the data catalogue has been addressed in Work Package 6. *Note: WP6 must be analysed to see what the GAPS are between both work packages.*

Within the scope of DAAMS, data users must have access to the catalogue and be able to create a request based on the selected, filtered, and linked datasets. Additionally, the DAAMS portal must enable data holders to update the catalogue, including the ability to publish or unpublish datasets. The catalogue is an integral part of the portal, providing seamless access to datasets while also supporting user authentication. The DAAMS portal supports both data requests and formal applications. Requests allow users to select and access datasets quickly for standard use cases, while applications involve a more detailed process that includes a formal approval workflow. Applications may also incur additional fees due to the extended processing requirements.

A full overview of the legal requirements of the catalogue is documented in WP6. While the legal requirements of this component are primarily related to WP6, for the sake of completeness they will be mentioned here as well. They concur with the following EHDS (version Nov 27, 2024) Articles: 57, 58, 60, 66, and 72.

This system supports the following core processes:

- Selection of data during request or application process;
- Starting a request or application based on data set selection;
- Publishing of new data sets/ remove from the HDC;
- Interaction between HDC and Data management & analytics, to track who uses what version of a dataset at what time.

The following legal requirements are part of this component *but are also included in the deliverable 6.1 of WP6*:

- **Requirement 2.43:** The datasets that are made available through the HDAB Health Data Catalogue (HDC) must all comply with an agreed set of minimal metadata. HDAB metadata quality standards should be applied and datasets offered must be held to those standards (EHDS art 57,58).

  Business process for this requirement: As part of the request the datasets for research may be looked up by entering keywords and other metadata in the HDC. This will be further determined in the HDC - work package 6.

- **Requirement 2.1:** The dataset details captured in the metadata or additional information attached to the dataset must contain information regarding their format and data sources where possible, including geographical coverage when data is requested from other member states (EHDS art 57 (1)(j)).

Business process for this requirement: Data holders must take care of the demanded minimum metadata set of their data and add these to the HDC.

- **Requirement 2.15:** By means of the metadata catalogue the data user will always be able to identify from which dataset a specific variable originates. In case of an enriched dataset, which is made available as part of the publication of the results of a research project, the information regarding the original dataset on which the enriched dataset was based must be made available, if this option is implemented in the Netherlands (EHDS art 57 (1)(j), 58 (1)).

  Business process for this requirement: The requestor can see the meta data of datasets up to the variable level.

- **Requirement 2.18:** HDAB must provide a catalogue function in which the data holders of all participating HDAB organisations publish their dataset (EHDS art 60 (3)).

  Business process for this requirement: Data holders must add meta data on their datasets for secondary use, both for 'originals' from primary use as well as for enriched datasets from HDAB research.

Now that the descriptions of the core components have been provided, we will turn to the supporting components. These supporting capabilities consist of non-functional processes and functions that enable and enhance the core application components of the DAAMS system.

Platform & Data Integration

Platform and Data integration refers to integration capabilities within the DAAMs system that connects an application to other applications, pushes or pulls HDAB-related procedural data from them, and orchestrates and executes workflows, among other things. This is commonly accomplished through APIs and webhooks to ensure smooth and efficient communication between systems.

This system supports the following core functions and processes:

- Data Mapping: connects and aligns data between systems;
- Integration Orchestration: coordinates data flow and system actions;
- Data Transformation: converts data formats for compatibility;
- Workflow Engine: automates key processes and tasks;
- Queuing Services: manages data in queues for efficient processing;
- App Connectors: links external applications to the platform;
- Scheduling: automates regular tasks and data transfers.

The following legal requirements are part of this component:
The EHDS does not stipulate legal requirements for this component, however the platform & data integration component ensures that other components function properly.

Platform Management

Platform management entails the technical back-office and organisational activities in managing the platform. Depending on the deployment scenario the technical services may be provided by a third party while HDAB maintains oversight.

The EHDS (version Nov 27, 2024) Articles pertaining to this component, and therefore the legal requirements, are (among others): 55, 57, 58, and 59.

This system supports the following core functions and processes:

- Organisational Tasks: overseeing administrative processes and resource planning;
- Technical Maintenance: performing updates, patches, and troubleshooting and communicating about these activities. This ensures transparency and keeps all stakeholders informed about planned and ongoing maintenance activities, minimizing disruptions;
- System Monitoring: tracking uptime, performance, and system health.

The following legal requirements are part of this component:

- **Requirement 6.1:** HDAB must ensure that there is sufficient capacity both in personnel and finances to support the management tasks HDAB is obligated to cover (EHDS 55(2)).

  Business process for this requirement: Management of the HDAB facilities (personnel, finances). For DAAMS, this specifically involves ensuring the technical and organisational sustainability of the system.

Data Management & Analytics

Data stored in the customer portal and case management system supports EHDS-compliant reporting.

The legal requirements presented as part of this supporting component relate to the following EHDS (version Nov 27, 2024) Articles : 55, 57, 58, 59, 60, 61, 68, 72 and 73.

This system supports the following core processes:

- Automated reporting;
- Custom data analysis: allows users to explore and analyse HDAB process-related data for specific needs;
- Self-service Business Intelligence: provides dashboards and visual tools for insights;
- Audit Trails: logs all data activities for compliance and transparency;
- Trend Analysis: tracks patterns in process-related data usage and performance.

The following legal requirements are part of this component:

- **Requirement 2.19:** HDAB must provide functionality with which any civilian/patient can inquire about the usage of their personal data. HDAB must publish methods on how data is processed within the HDAB platform and SPE (EHDS art. 58 (3)).

  Business process for this requirement: The use of every dataset is registered and summarised in published reports. The publication methods of the research for which the data set was used are also documented and published.

- **Requirement 2.25:** HDAB must inform the data holder of significant findings about individuals whose data has been processed (EHDS 58(3), 61(5)).

  Business process for this requirement: HDAB reports significant findings on an individual level to the data holder while ensuring privacy compliance.

- **Requirement 3.2:** HDAB must provide a biennial report on its operations, effectiveness and finances (EHDS art. 59 (1)).

  Business process for this requirement: The HDAB platform includes a system for generating and distributing (biennial) reports.

- **Requirement 4.2:** The HDAB must ensure transparency by publicly sharing descriptive information on all submitted data requests and applications, including their state, assessment, and results (EHDS art. 57 (1) (j)).

  Business process for this requirement: HDAB shares publicly detailed information on all submitted data requests and applications, including their status, assessment outcomes, and results.

- **Requirement 5.3:** HDAB must keep an audit trail of all health data access applications and usage of datasets as well as all activities within the HDAB environment. This must include (all) user actions and data manipulation activities done within the SPE (in consideration 68, art 73(3), indirect art 59 (1)(c) and (d) EHDS).

  Business process for this requirement: HDAB keeps track of which applications are submitted, and which data processing activities take place around and within the SPE.

Learning & Assessment

The capabilities in the learning and assessment component cover functionality involving awareness of users and assessing and mitigating activities on risks of health data exposure. Part of this could be an awareness course every data requester has to complete before access to data is granted.

The EHDS (version Nov 27, 2024) Articles pertaining to this component, and therefore the legal requirements, are (among others): 57, 59, 63, 68.

This system supports the following core processes:

- Awareness course;
- Providing course materials for onboarding and safe usage of HDAB and SPE services with focus on privacy;
- Management and certification of users that are trained and authorised to access data and HDAB services.

The following legal requirements are part of this component:

- **Requirement 4.10:** HDAB must establish that risks for defence, (public) safety and order, and the confidentiality of registration by supervisors, are weighed, either by HDAB or by external expertise (EHDS art. 68 (2)).

  Business process for this requirement: Security and confidentiality risks must be assessed and documented as part of HDAB procedures (this will be further developed by WP4).

- **Requirement 4.1:** The HDAB platform must safeguard the integrity of the use of data through policies that govern (EHDS art. 63, art. 52 (3) and (4) and art. 57 (1) c):
  - The prevention of any other use of the requested data than the one granted.
  - The protection of the rights of the data holder.
  - The protection of rights of the patient.

  Business process for this requirement: Security mechanisms must enforce strict access and usage policies for datasets.

- **Requirement 4.5**: The HDAB must share information regarding the usage of the platform with all active stakeholders (EHDS 59 (1a)).

  Business process for this requirement: HDAB fosters transparency and continuous improvement by sharing insights and usage statistics of the platform with active stakeholders.

Privacy and Security

A large part of the privacy and security processes are placed in WP7; for a complete overview WP7 should be consulted. In WP5 (DAAMs) the facilities that are necessary to implement, to monitor and to communicate with individuals, with government and with other stakeholders about security and privacy issues may be placed.

The legal requirements presented as part of this supporting component relate to the following EHDS (version Nov 27, 2024) Articles: 51, 53, 54, 55, 57, 58, 59, 60, 61, 66, 67, 68, 69, 71, 73, and 81.

This system supports the following core processes:

- Implementing privacy and security;
- Implementing opt-out registries
- Communicating privacy and security;
- Incident Management: responds to and resolves security breaches;
- Data Minimisation: limits data processing to only what is necessary.

The following legal requirements are part of this component:

- **Requirement 2.20:** Depending on how this is implemented in the Netherlands, HDAB may need to provide patients/citizens with the possibility of registering an opt-out. HDAB must manage the removal of data that is associated with a registered opt-out from its catalogue. (EHDS art. 71)

  Business process for this requirement: Depending on how this is implemented in the Netherlands, HDAB may need to provide patients/citizens the possibility to register an opt-out or provides a link to that register. HDAB manages the removal of data that is associated with a registered opt-out.

- **Requirement 2.28**: Enable logging of formal complaints. HDAB must on its platform provide functionality with which users, data holders, civilians/patients or other third parties can log a formal complaint (EHDS art. 81 (1) and (3)).

  Business process for this requirement: HDAB installs a complaint procedure for all types of participants and stakeholders, e.g. users, data holders, civilians/patients or other third parties.

- **Requirement 7.1:** HDAB is obligated to forward any complaints about the unfair use of data or the leaking of personal information directly with the Dutch DPA (Autoriteit Persoonsgegevens) (EHDS 81(4)).

  Business process for this requirement: HDAB organises that risk issues and complaints are registered and distributed to the Dutch DPA (Autoriteit Persoonsgegevens).

Governance and Compliance

This component encompasses functionalities to fill in certain governance and compliance capabilities. For WP5 (DAAMs) this entails not the actual governance tasks but the registry of these tasks. Other aspects related to governance and the coordination within HDAB-NL system will be covered by WP10.

The legal requirements of this supporting component pertain (at least) to the following EHDS (version Nov 27, 2024) Articles: 53, 55, 57,58, 59, 66, 68, 69, 71, and 73.

This system supports the following core processes:

- Registering governance tasks;
- Accountability of governance tasks**.**

The following legal requirements are part of this component:

- **Requirement 3.1:** HDAB must keep other HDABs within the HealthData@eu updated of its progress **(**EHDS art 57(1) (i)).

  Business process for this requirement: Progress updates on HDAB operations should be shared with HealthData@EU stakeholders.

- **Requirement 4.4:** HDAB must establish policies for the quality and state of the datasets the data holders intend to publish in the Health Data Catalogue (HDC), regarding data quality, privacy, data minimisation, completeness and a minimum set of meta data (EHDS art 66, 77-80).

  Business process for this requirement: HDAB stipulates policies and good practices that datasets published in the HDC meet defined quality and security standards by implementing clear policies.

- **Requirement 4.8**: HDAB ensures transparency by publishing clear policies on the required licenses and approvals for accessing and using its services (EHDS art. 57 par. 1 sub j).

  Business process for this requirement: HDAB ensures transparency by publishing clear policies on the required licenses and approvals for accessing and using its services.

- **Requirement 4.13:** HDAB will collaborate with the responsible authorities in the Netherlands regarding the implementation and compliance to applicable European and Dutch laws such as DGA, DA, MDR, IVDR, AIA, and the GDPR (EHDS art. 57 (2)(c)).

  Business process for this requirement: Collaboration frameworks should ensure compliance with national and EU regulations.

- **Requirement 4.14:** HDAB must comply with the organisational and operations responsibilities stated within the General Administrative Law (Algemene wet bestuursrecht).

Business process for this requirement: Compliance with administrative laws is integrated into HDAB policies and systems.

- **Requirement 4.17:** HDAB must involve and inform stakeholders regarding the definition and execution of its business strategy to ensure alignment of the needs of the stakeholders with the goals of the HDAB organisation (EHDS art 55 par 4 and art. 57 (2)(b)).

  Business process for this requirement: HDAB facilitates structured engagement with stakeholders by organising consultations, sharing strategic plans, and gathering feedback. This ensures that stakeholder needs are identified and aligned with the organisation's objectives, fostering transparency and trust.

- **Requirement 4.18:** HDAB must publish guidelines and policy defining acceptable use of the platform and SPE, as well as measures to prevent unfair use of data or misuse of the facilities HDAB offers (EHDS art 73(5)).

  Business process for this requirement: HDAB ensures transparency and accountability by providing clear guidelines and policies for all users of the HDAB platform and SPE. These documents define acceptable use, outline measures to prevent unfair data practices, and establish protocols to detect and address potential misuse.

- **Requirement 4.20:** HDAB shall assess if a health data request is complete and take into account the risks referred to in Article 69(2). HDAB shall assess the health data request within three months of receipt of the request and, where possible, subsequently provide the response to the health data user within a further three months (69.4).

  Business process for this requirement: HDAB ensures compliance with regulatory timelines by evaluating and deciding on requests as defined in the EHDS (article 53(1)). HDAB shall also provide the response within the regulatory period. Decisions are documented and communicated to ensure accountability and transparency.

  Requirement 4.21: HDAB must assess requests and applications based on the ethical use of the data and the purpose of the request or application based on guidelines provided within Dutch law. This includes assessment of a request or application when a patient opt-out cannot be honoured (EHDS art. 71 par 4 jo art. 68 par. 1 under g).

  Business process for this requirement: HDAB evaluates requests and applications to ensure these align with ethical standards and the legal framework. Requests and applications involving exceptions to patient opt-outs are reviewed to justify and document compliance with Dutch law and ethical principles.

- **Requirement 7.7**: HDAB must implement protective measures under the DGA Implementing Act for non-personal health data made available to a user outside EU jurisdiction and must take all reasonable technical, legal and organisational measures to prevent transfers of non-personal health data outside EU jurisdiction where this would conflict with national or European Union law (EHDS art. 88).

  Business process for this requirement: Organising rules and security systems around the use of data by non-EU users and transfer to non-EU territory.

Identity and Access Management

Identity and Access management (IAM) at DAAMs allows applying on behalf of an organisation, with authorisation managed by the organisation. The organisation's primary user(s) has(/have) visibility into all applications and decisions, and may add persons for specific roles. Data controllers have access to cost estimate and extraction requests and can provide comments. In the future, other authorities may also use the service.

This system supports the following core processes:

- User Login / Logout;
- Password Management: supports password resets and recovery;
- Access Control: assigns and manages user roles and permissions;
- User Management: adds, removes, or blocks user accounts;
- Activity Logging: tracks user actions for auditing and compliance;
- Verify user credentials.

The following legal requirements are part of this component:
The EHDS does not stipulate any legal requirements for this component.

Orchestration

Requests and applications, once submitted, flow into the case management system used by HDAB staff. Once a decision is made, application details, related discussions, attachments, and extraction descriptions are centrally available to personnel handling data compilation and processing. Status information of both applications and extractions, as well as the corresponding decisions, is shared from the case management system to the data user or data holder via the DAAMs portal. Requests for secure environments, billing, and related personnel are managed within the same system.

This system supports the following core processes:

- Orchestration of workflows and communication surrounding each workflow;
- Automatic provisioning of functionality, information and data based on workflow status.

The following legal requirements are part of this component:
There are no legal requirements for this component, however a smooth orchestration is essential for the timely delivering of decisions and permits.

9. Conclusion and next steps

This deliverable specified the functional legal requirements and specifications for the DAAMs. In 2025 and 2026, phase 2 will focus on completing this list with business and stakeholder requirements. This also means revisiting this deliverable and aligning (where necessary) with output from TEHDAS2 and HealthData@EU results. 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 WP5 team will keep involving the stakeholder community to ensure our solution is consistent with their needs and makes a positive impact on research in the Dutch Health Data landscape.

10. Appendices

Appendix 1: EHDS articles relevant for the DAAMs

Article 2 (second paragraph): definitions

t. '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, that has either: (i) the right or obligation, in accordance with applicable Union or national law and in its capacity as a controller or joint controller, to process personal electronic health data for the provision of healthcare or care or for the purposes of public health, reimbursement, research, innovation, policy making, official statistics or patient safety or for regulatory purposes; or (ii) the ability to make available non-personal electronic health data through the control of the technical design of a product and related services, including by registering, providing, restricting access to or exchanging such data;

Related hereto:

s. 'care' means a professional service the purpose of which is to address the specific needs of a natural person who, on account of impairment or other physical or mental conditions, requires assistance, including preventive and supportive measures, to carry out essential activities of daily living in order to support his or her personal autonomy;

b.) the definitions of 'healthcare', (….) laid down in Article 3, points (a), (c), (d), (f), (g), (i) and (k), respectively, of Directive 2011/24/EU;

u. '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;

Article 2, first paragraph

c. the definitions of 'data' (……..) and 'secure processing environment' laid down in Article 2, points (1), (13), (16), (17) and (20), respectively, of Regulation (EU) 2022/868;

From that regulation: article 2, point 1 (DGA):

'data' means any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording.

Data to be distinguished from (article 2, second paragraph EHDS):

w. 'dataset' means a structured collection of electronic health data;

x. ‘dataset of high impact for secondary use’ means a dataset the re-use of which is associated with significant benefits due to its relevance for health research;

Related to:

y. ‘dataset 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;

Which is different from:

v. ‘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;

Article 51 - Minimum categories of electronic health data for secondary use

1. Health data holders shall make the following categories of electronic health data available for secondary use in accordance with this Chapter:

a. electronic health data from EHRs;
b. data on factors impacting on health, including socio-economic, environmental and behavioural determinants of health;
c. aggregated data on healthcare needs, resources allocated to healthcare, the provision of and access to healthcare, healthcare expenditure and financing;
d. data on pathogens that impact human health;
e. healthcare-related administrative data, including on dispensations, reimbursement claims and reimbursements;
f. human genetic, epigenomic and genomic data;
g. other human molecular data such as proteomic, transcriptomic, metabolomic, lipidomic and other omic data;
h. personal electronic health data automatically generated through medical devices;
i. data from wellness applications;
j. data on professional status, and on the specialisation and institution of health professionals involved in the treatment of a natural person;
k. data from population-based health data registries such as public health registries;
l. data from medical registries and mortality registries;
m. data from clinical trials, clinical studies, clinical investigations and performance studies subject to Regulation (EU) No 536/2014, Regulation (EU) 2024/1938 of the European Parliament and of the Council 34, Regulation (EU) 2017/745 and Regulation (EU) 2017/746;
n. other health data from medical devices;
o. data from registries for medicinal products and medical devices;
p. data from research cohorts, questionnaires and surveys related to health, after the first publication of the related results;
q. health data from biobanks and associated databases.

2. Member States may provide in their national law that additional categories of electronic health data are to be made available for secondary use pursuant to this Regulation.

3. Member States may establish rules for the processing and use of electronic health data containing improvements related to the processing of those data, such as correction, annotation or enrichment, based on a data permit pursuant to Article 68.

4. Member States may introduce stricter measures and additional safeguards at national level aimed at safeguarding the sensitivity and value of the data that fall under paragraph 1, points (f), (g), (i) and (q). Member States shall notify the Commission of those measures and safeguards and, without delay, of any subsequent amendment affecting them.

Article 53 - Purposes for which electronic health data can be processed for secondary use

1. Health data access bodies shall only grant access to electronic health data referred to in Article 51 for secondary use to a health data user where the processing of the data by that health data user is necessary for one of the following purposes:

a. the public interest in the areas of public or occupational health, such as activities to protect against serious cross-border threats to health, public health surveillance or activities ensuring high levels of quality and safety of healthcare, including patient safety, and of medicinal products or medical devices;
b. policy-making and regulatory activities to support public sector bodies or Union institutions, bodies, offices or agencies, including regulatory authorities, in the health or care sector to carry out their tasks defined in their mandates;
c. statistics as defined in Article 3, point (1), of Regulation (EU) No 223/2009, such as national, multi-national and Union-level official statistics, related to health or care sectors;
d. education or teaching activities in health or care sectors at vocational or higher education level;
e. scientific research related to health or care sectors that contributes to public health or health technology assessments, or ensures high levels of quality and safety of healthcare, of medicinal products or of medical devices, with the aim of benefiting end-users, such as patients, health professionals and health administrators, including: (i) development and innovation activities for products or services; (ii) training, testing and evaluation of algorithms, including in medical devices, in vitro diagnostic medical devices, AI systems and digital health applications;
f. improvement of the delivery of care, of the optimisation of treatment and of the provision of healthcare, based on the electronic health data of other natural persons.

2. Access to electronic health data for the purposes referred to in paragraph 1, points (a), (b) and (c), shall be reserved for public sector bodies and Union institutions, bodies, offices and agencies exercising the tasks conferred on them by Union or national law, including where processing of data for carrying out those tasks is done by a third party on behalf of that public sector body or of Union institutions, bodies, offices and agencies.

Article 54 - Prohibited secondary use

Health data users shall only process electronic health data for secondary use on the basis of and in accordance with the purposes contained in a data permit issued pursuant to Article 68, health data requests approved pursuant to Article 69 or, in situations referred to in Article 67(3), an access approval from the relevant authorised participant in HealthData@EU referred to in Article 75. In particular, seeking access to and processing electronic health data obtained via a data permit issued pursuant to Article 68 or a health data request approved pursuant to Article 69 for the following uses shall be prohibited:

a. taking decisions detrimental to a natural person or a group of natural persons based on their electronic health data; in order to qualify as 'decisions' for the purposes of this point, they have to produce legal, social or economic effects or similarly significantly affect those natural persons;
b. taking decisions in relation to a natural person or a group of natural persons in relation to job offers, offering less favourable terms in the provision of goods or services, including exclusion of such persons or groups from the benefit of an insurance or credit contract, the modification of their contributions and insurance premiums or conditions of loans, or taking any other decisions in relation to a natural person or a group of natural persons which result in discriminating against them on the basis of the health data obtained;
c. carrying out advertising or marketing activities;
d. developing products or services that may harm individuals, public health or society at large, such as illicit drugs, alcoholic beverages, tobacco and nicotine products, weaponry or products or services which are designed or modified in such a way that they create addiction, contravene public order or cause a risk for human health;
e. carrying out activities in conflict with ethical provisions laid down in national law.

Article 55 - Health data access bodies

1. Member States shall designate one or more health data access bodies responsible for carrying out the tasks and obligations set out in Articles 57, 58 and 59. Member States may either establish one or more new public sector bodies or rely on existing public sector bodies or on internal services of public sector bodies that fulfil the conditions set out in this Article. The tasks set out in Article 57 may be distributed between different health data access bodies. Where a Member State designates several health data access bodies, it shall designate one health data access body to act as coordinator, with responsibility for coordinating tasks with the other health data access bodies both within the territory of that Member State and in other Member States. Each health data access body shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, health data access bodies shall cooperate with each other, with the Commission and, for concerns regarding data protection, with the relevant supervisory authorities.

Article 57 - Tasks of health data access bodies

1. Health data access bodies shall carry out the following tasks:

a. deciding on health data access applications pursuant to Article 67 of this Regulation, authorising and issuing data permits pursuant to Article 68 of this Regulation to access electronic health data falling within their remit for secondary use and deciding on health data requests submitted pursuant to Article 69 of this Regulation in accordance with this Chapter and Chapter II of Regulation (EU) 2022/868, including with regard to: (i) providing access to electronic health data to health data users pursuant to a data permit in a secure processing environment in accordance with Article 73; (ii) monitoring and supervising compliance by health data users and health data holders with the requirements laid down in this Regulation; (iii) requesting electronic health data referred to in Article 51 from relevant health data holders pursuant to a data permit issued or a health data request approved;
b. processing electronic health data referred to in Article 51 such as by receiving, combining, preparing and compiling such data when requested from health data holders and the pseudonymisation or anonymisation of those data;
c. taking all measures necessary to preserve the confidentiality of intellectual property rights, for regulatory data protection and to preserve the confidentiality of trade secrets as provided for in Article 52, taking into account the relevant rights of both the health data holder and health data user;
d. cooperating with and supervising health data holders to ensure the consistent and accurate implementation of the provisions on data quality and utility label in Article 78;
e. maintaining a management system to record and process health data access applications, health data requests, decisions on those applications and requests and the data permits issued and health data requests handled, providing at least information on the name of the health data applicant, the purpose of access, the date of issuance, the duration of the data permit and a description of the health data access application or the health data request;
f. maintaining a public information system to comply with the obligations laid down in Article 58;
g. cooperating at Union and national level to lay down common standards, technical requirements and appropriate measures for accessing electronic health data in a secure processing environment;
h. cooperating at Union and national level and providing advice to the Commission on techniques and best practices for secondary use and the management of electronic health data;
i. facilitating cross-border access to electronic health data for secondary use hosted in other Member States through HealthData@EU referred to in Article 75 and cooperating closely with each other and with the Commission;
j. making public, through electronic means: (i) a national dataset catalogue that includes details about the source and nature of electronic health data, in accordance with Articles 77, 78 and 80, and the conditions for making electronic health data available; (ii) any health data access application and health data request without undue delay after initial reception; (iii) all data permits issued or health data requests approved as well as refusal decisions, including their justification, within 30 working days of the issuance, approval or refusal; (iv) measures related to non-compliance pursuant to Article 63; (v) results communicated by health data users pursuant to Article 61(4); (vi) an information system to comply with the obligations laid down in Article 58; (vii) information, at a minimum on an easily accessible website or web portal, on the connection to HealthData@EU of national contact points for secondary use of a third country, or of a system established at international level by an international

organisation, as soon as the third country or the international organisation becomes an authorised participant in HealthData@EU.

Article 58 - Obligations of health data access bodies towards natural persons

1. Health data access bodies shall make information on the conditions under which electronic health data are made available for secondary use publicly available, easily searchable through electronic means and accessible for natural persons. That information shall cover the following:

a. the legal basis under which access to electronic health data is granted to the health data user;
b. the technical and organisational measures taken to protect the rights of natural persons;
c. the applicable rights of natural persons in relation to secondary use;
d. the arrangements for natural persons to exercise their rights in accordance with Chapter III of Regulation (EU) 2016/679;
e. the identity and the contact details of the health data access body;
f. who has been granted access to datasets of electronic health data and to which datasets they were granted access and details of the data permit regarding the purposes for processing such data as referred to in Article 53(1);
g. the results or outcomes of the projects for which the electronic health data were used.

2. 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.

3. Where a health data access body is informed by a health data user of a significant finding related to the health of a natural person, as referred to in Article 61(5), the health data access body shall inform the health data holder about that finding. The health data holder shall, under the conditions laid down by national law, inform the natural person or health professional treating the natural person concerned. Natural persons shall have the right to request not to be informed of such findings.

4. Member States shall inform the public at large about the role and benefits of health data access bodies.

Article 59 - Reporting by health data access bodies

1. Each health data access body shall publish an activity report every two years and make it publicly available on its website. If a Member State designates more than one health data access body, the coordinating body referred to in Article 55(1) shall be responsible for the activity report and request the necessary information from the other health data access bodies. That activity report shall follow a structure agreed by the EHDS Board pursuant to Article 94(2), point (d), and contain at least the following categories of information:

a. information relating to the health data access applications and health data requests submitted, such as the types of health data applicants, number of data permits issued or

refused, categories of purposes of access and categories of electronic health data accessed, and a summary of the results of the electronic health data uses, where applicable;

b. information on the fulfilment of regulatory and contractual commitments by health data users and health data holders, as well as the number and amount of administrative fines imposed by health data access bodies;
c. information on audits carried out on health data users to ensure compliance of the processing they carry out in the secure processing environment pursuant to Article 73(1), point (e);
d. information on internal and third party audits on compliance of secure processing environments with the defined standards, specifications and requirements, as referred to in Article 73(3);
e. information on the handling of requests from natural persons relating to the exercise of their data protection rights;
f. a description of the health data access body's activities carried out in relation to engagement with and consultation of relevant stakeholders;
g. revenues from data permits and health data requests;
h. the average number of days between health data access applications or health data requests and access to data;
i. the number of data quality labels issued by health data holders, disaggregated per quality category;
j. the number of peer-reviewed research publications, policy documents and regulatory procedures using data accessed via the EHDS;
k. the number of digital health products and services, including AI applications, developed using data accessed via the EHDS.

2. The activity report referred to in paragraph 1 shall be submitted to the Commission and the EHDS Board within six months of the end of the second year of the relevant reporting period. The activity report shall be accessible via the Commission's website.

Article 60 - Duties of health data holders

1. Health data holders shall make relevant electronic health data referred to in Article 51 available upon request to the health data access body, in accordance with a data permit issued pursuant to Article 68, or upon a health data request approved pursuant to Article 69.

2. Health data holders shall put the requested electronic health data referred to in paragraph 1 at the disposal of the health data access body within a reasonable time and no later than three months from the receipt of the request by the health data access body. In justified cases, the health data access body may extend that period by a maximum of three months.

3. The health data holder shall communicate to the health data access body a description of the dataset it holds in accordance with Article 77. The health data holder shall, at a minimum on an annual basis, check that its dataset description in the national dataset catalogue is accurate and up to date.

4. Where a data quality and utility label accompanies the dataset pursuant to Article 78, the health data holder shall provide sufficient documentation to the health data access body for that body to verify the accuracy of the label.

5. Health data holders of non-personal electronic health data shall provide access to data through trusted open databases to ensure unrestricted access for all users and data storage and preservation. Trusted open public databases shall have in place robust, transparent and sustainable governance and a transparent model of user access.

Article 61 - Duties of health data users

1. 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 pursuant to Article 68, a health data request approved pursuant to Article 69 or, in situations referred to in Article 67(3), an access approval from the relevant authorised participant in HealthData@EU referred to in Article 75.

2. When processing electronic health data within the secure processing environments referred to in Article 73, health data users shall not provide access to the electronic health data, or make those data available, to third parties not mentioned in the data permit.

3. Health data users shall not re-identify or attempt to re-identify the natural persons to whom the electronic health data obtained by the health data users on the basis of a data permit, a health data request or an access approval by an authorised participant in HealthData@EU relate.

4. Health data users shall make public the results or output of secondary use, including information relevant for the provision of healthcare, within 18 months of the completion of the processing of the electronic health data in the secure processing environment or of having received the response to the health data request referred to in Article 69. In justified cases related to the permitted purposes of the processing of electronic health data, the period referred to in the first subparagraph may be extended by the health data access body, in particular in cases where the result is published in a scientific journal or other scientific publication. The results or output of secondary use shall contain only anonymous data. Health data users shall inform the health data access bodies from which a data permit was obtained about the results or output of secondary use and assist them to make that information public on health data access bodies' websites. Such publication shall be without prejudice to publication rights in scientific journals or other scientific publications. When health data users use electronic health data in accordance with this Chapter, they shall acknowledge the sources of the electronic health data and the fact that the electronic health data have been obtained in the framework of the EHDS.

5. Without prejudice to paragraph 2, health data users shall inform the health data access body of any significant finding related to the health of the natural person whose data are included in the dataset.

6. Health data users shall cooperate with health data access bodies in those bodies' performance of their tasks.

Article 62 - Fees

1. Health data access bodies, including the Union health data access service, or trusted health data holders referred to in Article 72 may charge fees for making electronic health data available for secondary use. The fees shall be in proportion to the cost of making the data available and they shall not restrict competition. The fees shall cover all or part of the costs related to the procedure for assessing a health data access application or a health data request, for issuing, refusing or amending a data permit pursuant to Articles 67 and 68 or for providing a response to a health data request submitted pursuant to Article 69, including costs related to the consolidation, preparation, pseudonymisation, anonymisation and provision of the electronic health data. Member States may establish reduced fees for certain types of health data users located in the Union, such as public sector bodies or Union institutions, bodies, offices and agencies with a legal mandate in the field of public health, university researchers or microenterprises.

2. The fees referred to in paragraph 1 of this Article may include compensation for the costs incurred by the health data holder for compiling and preparing the electronic health data to be made available for secondary use. In such cases, the health data holder shall provide an estimate of such costs to the health data access body. Where the health data holder is a public sector body, Article 6 of Regulation (EU) 2022/868 shall not apply. The part of the fees linked to the health data holder's costs shall be paid to the health data holder.

3. Any fees charged to health data users pursuant to this Article shall be transparent and non-discriminatory.

4. Where health data holders and health data users do not agree on the level of the fees within one month of the data permit being issued, the health data access body may set the fees in proportion to the cost of making electronic health data available for secondary use. Where health data holders or health data users disagree with the fee set by the health data access body, they shall have access to dispute settlement bodies in accordance with Article 10 of Regulation (EU) 2023/2854.

5. Before issuing a data permit pursuant to Article 68 or providing a response to a health data request submitted pursuant to Article 69, the health data access body shall inform the health data applicant of the estimated fees. The health data applicant shall be informed about the option to withdraw the health data access application or health data request. If the health data applicant withdraws its application or request, the health data applicant shall only be charged the costs that have already been incurred. 6. The Commission shall, by means of implementing acts, lay down principles for the fee policies and fee structures, including deductions for the entities referred to in paragraph 1, fourth subparagraph, of this Article in order to support consistency and transparency between Member States regarding such fee policies and fee structures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 98(2).

Article 66 - Data minimisation and purpose limitation

1. Where health data access bodies receive a health data access application, they shall ensure that access is only provided to electronic health data that are adequate, relevant and limited to what is necessary in relation to the purpose of processing indicated in the health data access application by the health data user and in line with the data permit issued pursuant to Article 68.

2. Health data access bodies 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, taking into account the information provided by the health data user.

3. 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), health data access bodies shall provide access to electronic health data in pseudonymised format. The information necessary to reverse the pseudonymisation shall be available only to the health data access body or an entity that acts as a trusted third party in accordance with national law.

Article 67 - Health data access applications

1. A natural or legal person may submit a health data access application for the purposes referred to in Article 53(1) to a health data access body.

2. The health data access application shall include:

a. the health data applicant's identity, a description of that health data applicant's professional functions and activities, including the identity of the natural persons who would have access to the electronic health data if a data permit were issued; the health data applicant shall notify the health data access body of any update of the list of natural persons;
b. the purposes referred to in Article 53(1) for which access to data is applied for;
c. a detailed explanation of the intended use of the electronic health data and expected benefit related to that use and how that benefit would contribute to the purposes referred to in Article 53(1);
d. a description of the requested electronic health data, including their scope, time range, format, sources and, where possible, the geographical coverage where such data are requested from health data holders in several Member States or from authorised participants in HealthData@EU referred to in Article 75;
e. a description explaining whether the electronic health data need to be made available in a pseudonymised or anonymised format; in the case of a pseudonymised format, a justification as to why the processing cannot be carried out using anonymised data;
f. where the health data applicant intends to bring datasets already held by that health data applicant into the secure processing environment, a description of those datasets;
g. a description of the safeguards, which are to be proportionate to the risks, planned to prevent any misuse of the electronic health data, as well as to protect the rights and interests of the health data holder and of the natural persons concerned, including to prevent any re-identification of natural persons in the dataset;
h. a justified indication of the period during which the electronic health data are needed for processing in a secure processing environment;
i. a description of the tools and computing resources needed for a secure processing environment;
j. where applicable, information on any assessment of ethical aspects of the processing, required under national law, which may serve to replace the health data applicant's own ethics assessment;
k. where the health data applicant intends to make use of an exception under Article 71(4), the justification required by national law pursuant to that Article.

3. When seeking access to electronic health data held by health data holders established in more than one Member State or from the relevant authorised participants in HealthData@EU referred to in Article 75, the health data applicant shall submit a single health data access application through the health data access body of the Member State where the main establishment of the health data applicant is located, through the health data access body of the Member State in which one of those health data holders is established or through the services provided by the Commission in HealthData@EU referred to in Article 75. The health data access application shall be automatically forwarded to the relevant authorised participants in HealthData@EU and to the health data access bodies of the Member States where the health data holders identified in the health data access application are established.

4. When seeking access to the personal electronic health data in a pseudonymised format, the health data applicant shall provide, together with the health data access application, a description of how the processing would comply with applicable Union and national law on data protection and privacy, in particular with Regulation (EU) 2016/679 and, more specifically, with Article 6(1) thereof.

Article 68 - Data permit

1. For the purposes of granting access to electronic health data, the health data access bodies shall assess whether all the following criteria are fulfilled:

a. the purposes described in the health data access application correspond to one or more of the purposes listed in Article 53(1);
b. the requested data are necessary, adequate and proportionate for the purposes described in the health data access application, taking into account data minimisation and purpose limitation requirements provided for in Article 66;
c. the processing complies with Article 6(1) of Regulation (EU) 2016/679 and, in the case of pseudonymised data, there is sufficient justification that the purpose cannot be achieved with anonymised data;
d. the health data applicant is qualified in relation to the intended purposes of data use and has appropriate expertise, including professional qualifications in the areas of healthcare, care, public health or research, consistent with ethical practice and applicable laws and regulations;
e. the health data applicant demonstrates sufficient technical and organisational measures to prevent the misuse of the electronic health data and to protect the rights and interests of the health data holder and of the natural persons concerned;
f. the information on the assessment of ethical aspects of the processing, referred to in Article 67(2), point (j), where applicable, complies with national law;
g. where the health data applicant intends to make use of an exception under Article 71(4), the justification required by national law adopted pursuant to that Article has been provided;
h. all other requirements in this Chapter are fulfilled by the health data applicant.

2. The health data access body shall also take into account the following:

a. risks for national defence, security, public security and public order;

b. the risk of undermining the confidentiality of data in governmental databases of regulatory authorities.

3. Where the health data access body concludes that the requirements in paragraph 1 are fulfilled and the risks referred to in paragraph 2 are sufficiently mitigated, the health data access body shall grant access to electronic health data by issuing a data permit. Health data access bodies shall refuse all health data access applications where the requirements in this Chapter are not fulfilled. Where the requirements for issuing a data permit are not met, but the requirements to provide a response in an anonymised statistical format under Article 69 are, the health data access body may decide to provide such response, on condition that providing that response would mitigate the risks and, if the purpose of the health data access application can be fulfilled in this manner, that the health data applicant agrees to receiving a response in an anonymised statistical format under Article 69.

4. By way of derogation from Regulation (EU) 2022/868, the health data access body shall issue or refuse a data permit within three months of receiving a complete health data access application. If the health data access body finds that the health data access application is incomplete, it shall notify the health data applicant, who shall be given the possibility of completing that application. If the health data applicant does not complete the health data access application within four weeks, the data permit shall not be issued. The health data access body may extend the period for responding to a health data access application by three additional months where necessary, taking into account the urgency and complexity of the health data access application and the volume of health data access applications submitted for decision. In such cases, the health data access body shall notify the health data applicant as soon as possible that more time is needed for examining the health data access application, together with the reasons for the delay.

5. When handling a health data access application for cross-border access to electronic health data referred to in Article 67(3), health data access bodies and relevant authorised participants in HealthData@EU referred to in Article 75 shall remain responsible for adopting decisions to grant or refuse access to electronic health data within their remit in accordance with this Chapter. The health data access bodies and authorised participants in HealthData@EU concerned shall inform each other of their decisions. They may take that information into consideration when deciding on granting or refusing access to electronic health data. A data permit issued by one health data access body may benefit from mutual recognition by the other health data access bodies.

6. Member States shall provide for an accelerated health data access application procedure for public sector bodies and Union institutions, bodies, offices and agencies with a legal mandate in the field of public health if the processing of electronic health data is to be carried out for the purposes established in Article 53(1), points (a), (b) and (c). When such accelerated procedure applies, the health data access body shall issue or refuse a data permit within two months of receiving a complete health data access application. The health data access body may extend the period for responding to a health data access application by one additional month where necessary.

7. Following the issuance of the data permit, the health data access body shall immediately request the electronic health data from the health data holder. The health data access body shall make available the electronic health data to the health data user within two months of receiving them from the health data holders, unless the health data access body specifies that the data are to be provided within a longer specified timeframe.

8. In cases referred to in paragraph 5, first subparagraph, the health data access bodies and authorised participants in HealthData@EU which issued a data permit or access approval, respectively, may decide to provide access to the electronic health data in the secure processing environment provided by the Commission as referred to in Article 75(9).

9. Where the health data access body refuses to issue a data permit, it shall provide a justification for that refusal to the health data applicant.

10. When issuing a data permit, the health data access body shall set out in that data permit the general conditions applicable to the health data user. The data permit shall contain the following:

a. the categories, specification and format of the electronic health data to be accessed, which are covered by the data permit, including their sources and an indication of whether the electronic health data are to be accessed in a pseudonymised format in the secure processing environment;
b. a detailed description of the purpose for which the electronic health data are made available;
c. where a mechanism to implement an exception is provided for and applicable under Article 71(4), information on whether it has been applied and the reason for the related decision;
d. the identity of authorised persons, in particular the identity of the principal investigator, with access rights to the electronic health data in the secure processing environment;
e. the duration of the data permit;
f. information about the technical characteristics and tools available to the health data user within the secure processing environment;
g. the fees to be paid by the health data user;
h. any specific conditions.

11. Health data users shall have the right to access and process the electronic health data in a secure processing environment in accordance with the data permit issued to them on the basis of this Regulation.

12. A data permit shall be issued for the duration necessary to fulfil the requested purposes and that duration shall not exceed 10 years. That duration may be extended once for a period which does not exceed 10 years, at the request of the health data user, based on arguments and documents to justify that extension which shall be provided one month before the expiry of the data permit. The health data access body may charge fees which increase to reflect the costs and risks of storing electronic health data for a period exceeding the initial period. In order to reduce such costs and fees, the health data access body may also propose to the health data user to store the dataset in a storage system with reduced capabilities. Such reduced capabilities shall not affect the security of the processed dataset. The electronic health data within the secure processing environment shall be deleted within six months of the expiry of the data permit. At the request of the health data user, the formula for the creation of the requested dataset may be stored by the health data access body.

13. If the data permit needs to be updated, the health data user shall submit a request for an amendment of the data permit.

Article 69 - Health data request

1. The health data applicant may submit a health data request for the purposes referred to in Article 53 with the aim of obtaining a response only in an anonymised statistical format. A health data access body shall not provide a response to a health data request in any other format and the health data user shall have no access to the electronic health data used to provide that response.

2. A health data request as referred to in paragraph 1 shall include the following information:

a. the identity of the health data applicant and a description of that health data applicant's professional functions and activities;
b. a detailed explanation of the intended use of the electronic health data, including the purposes referred to in Article 53(1) for which the health data request is submitted;
c. a description of the requested electronic health data, their format and the sources of those data, where possible;
d. a description of the statistical content;
e. a description of the safeguards planned to prevent any misuse of the requested electronic health data;
f. a description of how the processing would comply with Article 6(1) of Regulation (EU) 2016/679 or Article 5(1) and Article 10(2) of Regulation (EU) 2018/1725;
g. where the health data applicant intends to make use of an exception under Article 71(4), the justification required in that regard by national law pursuant to that Article.

3. The health data access body shall assess if the health data request is complete and take into account the risks referred to in Article 68(2).

4. The health data access body shall assess the health data request within three months of receipt of the request and, where possible, subsequently provide the response to the health data user within a further three months.

Article 70 - Templates to support access to electronic health data for secondary use

By ... [two years from the date of entry into force of this Regulation], the Commission shall, by means of implementing acts, set out the templates for the health data access application, the data permit and the health data request referred to in Articles 67, 68 and 69, respectively. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 98(2).

Article 71 - Right to opt out from the processing of personal electronic health data for secondary use

1. Natural persons shall have the right to opt out at any time, and without providing any reason, from the processing of personal electronic health data relating to them for secondary use under this Regulation. The exercise of that right shall be reversible.

2. Member States shall provide for an accessible and easily understandable opt-out mechanism to exercise the right established in paragraph 1, whereby natural persons may explicitly state that they do not wish to have their personal electronic health data processed for secondary use.

3. Once natural persons have exercised the right to opt out, and where personal electronic health data relating to them can be identified in a dataset, personal electronic health data relating to those

natural persons shall not be made available or otherwise processed pursuant to data permits issued under Article 68 or health data requests under Article 69 approved after the natural person has exercised the right to opt out. The first subparagraph of this paragraph shall not affect the processing for secondary use of personal electronic health data relating to those natural persons pursuant to data permits or health data requests that were issued or approved before the natural persons exercised their right to opt out.

4. By way of exception from the right to opt out provided for in paragraph 1, a Member State may provide in its national law for a mechanism to make data for which a right to opt out has been exercised available provided that all the following conditions are fulfilled:

a. the health data access application or health data request is submitted by a public sector body or a Union institution, body, office or agency with a mandate to carry out tasks in the area of public health, or by another entity entrusted with carrying out public tasks in the area of public health, or acting on behalf of or commissioned by a public authority, and the processing of those data is necessary for any of the following purposes: (i) the purposes referred to in Article 53(1), points (a), (b) and (c); (ii) scientific research for important reasons of public interest;
b. those data cannot be obtained by alternative means in a timely and effective manner under equivalent conditions;
c. the health data applicant has provided the justification referred to in Article 68(1), point (g), or in Article 69(2), point (g). The national law providing for such a mechanism shall provide for specific and suitable measures in order to protect the fundamental rights and the personal data of natural persons. Where a Member State has provided in its national law for the possibility to request access to data for which a right to opt out has been exercised and the conditions referred to in the first subparagraph of this paragraph are fulfilled, those data may be included when carrying out the tasks under Article 57(1), points (a)(i), (a)(iii) and (b).

5. The rules on any mechanism to implement exceptions provided for under paragraph 4 by way of exception from paragraph 1 shall respect the essence of the fundamental rights and freedoms and shall be a necessary and proportionate measure in a democratic society to fulfil purposes of public interest in the area of legitimate scientific and societal objectives.

6. Any processing carried out in accordance with a mechanism to implement exceptions provided for under paragraph 4 of this Article shall comply with the requirements of this Chapter, in particular the prohibition on re-identifying or attempting to re-identify natural persons in accordance with Article 61(3). Any legislative measure providing for a mechanism in national law as referred to in paragraph 4 of this Article shall include specific provisions for the safety, and the protection of the rights, of natural persons.

7. Member States shall notify without delay the Commission of the provisions of their national law which they adopt pursuant to paragraph 4 and of any subsequent amendment affecting them.

8. When the purposes of the processing of personal electronic health data by a health data holder do not or no longer require the identification of a data subject by the controller, that health data holder shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with the right to opt out under this Article.

Article 72 - Simplified procedure for access to electronic health data from a trusted health data holder

1. Where a health data access body receives a health data access application pursuant to Article 67 or a health data request pursuant to Article 69 that only covers electronic health data held by a trusted health data holder designated in accordance with paragraph 2 of this Article, the procedure set out in paragraphs 4 to 6 of this Article shall apply.

2. Member States may establish a procedure whereby health data holders can apply to be designated as trusted health data holders, provided the health data holders meet the following conditions:

a. they are able to provide access to health data through a secure processing environment that complies with Article 73;
b. they have the necessary expertise to assess health data access applications and health data requests;
c. they provide the necessary guarantees to ensure compliance with this Regulation. Member States shall designate trusted health data holders following an assessment of the fulfilment of those conditions by the relevant health data access body. Member States shall establish a procedure to regularly review whether the trusted health data holder continues to fulfil those conditions. Health data access bodies shall indicate the trusted health data holders in the dataset catalogue referred to in Article 77.

3. Health data access applications and health data requests referred to in paragraph 1 shall be submitted to the health data access body, which may forward them to the relevant trusted health data holder.

4. Following receipt of a health data access application or health data request pursuant to paragraph 3 of this Article, the trusted health data holder shall assess the health data access application or health data request against the criteria listed in Article 68(1) and (2) or Article 69(2) and (3), as applicable.

5. The trusted health data holder shall submit the assessment it carries out pursuant to paragraph 4, accompanied by a proposal for decision, to the health data access body within two months of receipt of the health data access application or health data request from the health data access body. Within two months of receipt of the assessment, the health data access body shall issue a decision on the health data access application or health data request. The health data access body shall not be bound by the proposal submitted by the trusted health data holder.

6. Following the health data access body's decision to issue the data permit or to approve the health data request, the trusted health data holder shall carry out the tasks referred to in Article 57(1), points (a)(i) and (b).

7. The Union health data access service referred to in Article 56 may designate health data holders that are Union institutions, bodies, offices or agencies which comply with the conditions laid down in paragraph 2, first subparagraph, points (a), (b) and (c), of this Article as trusted health data holders. Where it does so, paragraph 2, third and fourth subparagraphs, and paragraphs 3 to 6 of this Article shall apply mutatis mutandis.

Article 73 - Secure processing environment

1. 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. In particular, the secure processing environment shall comply with the following security measures:

a. the restriction of access to the secure processing environment to authorised natural persons listed in the data permit issued pursuant to Article 68;
b. the minimisation of 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;
c. the limitation of 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;
d. ensuring 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 only;
e. the keeping of identifiable logs of access to and activities in the secure processing environment for the period necessary to verify and audit all processing operations in that environment; logs of access shall be kept for at least one year;
f. ensuring compliance and monitoring the security measures referred to in this paragraph to mitigate potential security threats.

2. 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 secure processing environment. 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 nonpersonal electronic health data, including electronic health data in an anonymised statistical format, from the secure processing environment.

3. Health data access bodies shall ensure that audits of the secure processing environments are carried out on a regular basis, including by third parties, and shall take corrective action for any shortcomings, risks or vulnerabilities identified by those audits in the secure processing environments.

4. Where recognised data altruism organisations under Chapter IV of Regulation (EU) 2022/868 process personal electronic health data using a secure processing environment, those environments shall also comply with the security measures set out in paragraph 1, points (a) to (f), of this Article.

5. 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. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 98(2).

Article 81 - Right to lodge a complaint with a health data access body

1. Without prejudice to any other administrative or judicial remedy, natural and legal persons shall have the right to lodge a complaint in relation to the provisions laid down in this Chapter, individually or, where relevant, collectively, with a health data access body, provided that their rights or interests are negatively affected.

2. The health data access body with which the complaint has been lodged shall inform the complainant of the progress made in dealing with the complaint and of the decision taken on the complaint.

3. Health data access bodies shall provide easily accessible tools for the submission of complaints.

4. Where the complaint concerns the rights of natural persons pursuant to Article 71 of this Regulation, the complaint shall be transmitted to the competent supervisory authority under Regulation (EU) 2016/679. The relevant health data access body shall provide the necessary information at its disposal to that supervisory authority under Regulation (EU) 2016/679 in order to facilitate the assessment and investigation of the complaint.

Appendix 2: Table for MS 5.1.2

A first baseline overview (developed in Q1-Q2 of 2024) with core components and their functionalities as described in the concept version of the EHDS text (March 2024). Some functionalities are found in multiple core components.

Core component	Functionality according to the EHDS	Associated EHDS articles (version March 2024)
Requesting	Receive and transmit metadata	37(1)(k)(q)
Processing	Financial services Apply sovereignty restrictions Check and/or execute application assessment Review and determination of invoices Trusted data holder management Granting of permits Collecting, preparing, making the data available for use Permit management DAAMs system must include cooperation with the HDAB, (= separate, but parallel process) which makes the legal decision	37(1)(a)(d)(f); 42; 44; 45; 46; 49(2)(4); 50(2); 60aa; 61; 62
Informing	Providing information about applications and processing Providing public information about applications and processing Operational report Feedback relevant findings to data holder Granting of permits Complaint handling Appeal and objection	37(1)(q)(r); 37(1)a; 37(3); 39; 45; 46; 68a
Registration	Appeal and objection Compliance Complaint handling Operational report	39; 68a

Appendix 3: Table for MS 5.1.1

An overview of existing DAAMs solutions and components

#	System name and/or organisation name, and region	Request	Processing	Informing	Registration
1	REMS, Statistics Finland, FI	Request form Data list including 'terms of use' OpenID connect. (EHDS meta data receive and transmit).	Assessment Committee ('DAC') Data list incl. assessment committee. Check and/or carry out assessment of application. (Complies with EHDS functionality: Permit granting).	Providing individual information regarding requests and processing. (Complies with EHDS functionality: Permit granting).	Complete logs (i.e. for audit purposes).
2	Microdataservices, CBS, NL, CBS, NL	Self Service Counter, for authorisation requests; and data requests (per research project).	Financial services. Check and/or carry out application assessment. Reviewing and determining invoices. Trusted data holder management. Licensing (at institution and researcher level). Collecting, preparing, making available and unlocking data for use. Management of license.	Providing information about applications and processing. Providing public information about applications and processing. Operational reporting.	Complete logs (i.e. for audit purposes).
3	Statistics Denmark, DK	Receive and transmit meta data.	Financial Services. Check and/or carry out assessment of application. Review and determination of invoices. Granting of permits. Collecting, preparing, and unlocking data for use.	Providing individual information regarding requests and processing. Granting of permits.	
4	Research Manager, PMC, NL		Check and/or carry out application assessment.		

5	Microsoft Dynamics, IKNL, NL		Financial Services. Check and/or carry out assessment of application. Review and determination of invoices. Granting of permits. Collecting, preparing, and unlocking data for use.	Providing individual information regarding requests and processing. Operational reporting. Granting of permits.	
6	Health-RI Request Tool, NL	Dataset selected from meta data catalogue will be redirected to a request form.	Request portal to facilitate the request process. Contract management services.	To be decided.	Request registry.
7	Belgian Health Data Agency, BE	Data request form through the web-portal	Steps: 1. Analysis of the application; 2. Assessment of the application; 3. Notification of decision; 4. Preparation of datasets and meta data; 5. Quality assurance; 6. Data access. Summarised in a pdf.		
8	Helsedataservice, NO	Receive and transmit meta data	Financial Services. Check and/or carry out assessment of application. Review and determination of invoices. Granting of permits. Collecting, preparing, and unlocking data for use.	Providing individual information regarding requests and processing.	

Appendix 4: Functional legal requirements based on the EHDS (version December 2024)

Req. ID	Req. Title & Description	Business Component	Business Process	Functional Requirement Description	Articles
REQ. 2.1	The dataset details captured in the metadata or additional information attached to the dataset must contain information regarding their format and data sources where possible, including geographical coverage when data is requested from other member states.	Catalogue Service	Data holders must take care of the demanded minimum metadata set of their data and add these to the HDC.	The elaboration of these requirements will be coordinated with WP6	EHDS art 57 (1)(j)
REQ. 2.15	By means of the metadata catalogue the data user will always be able to identify from which dataset a specific variable originates. In case of an enriched dataset, which is made available as part of the publication of the results of a research project, the information regarding the original dataset on which the enriched dataset was based must be made available.	Catalogue Service	The requestor can see the meta data of datasets up to the variable level.	The elaboration of these requirements will be coordinated with WP6	EHDS art 57 (1)(j), 58 (1)
REQ. 2.18	HDAB must provide a catalogue function in which the data holders of all participating HDAB organisations publish their dataset.	Catalogue Service	Data holders must add meta data on their datasets for secondary use, both for 'originals' from primary use as well as for enriched datasets from HDAB research.	The elaboration of these requirements will be coordinated with WP6	EHDS art 60 (3)

REQ. 2.43	The datasets that are made available through the HDAB Health Data Catalogue (HDC) must all comply with an agreed set of minimal metadata. HDAB metadata quality standards should be applied and datasets offered must be held to those standards.	Catalogue Service	As part of the request the datasets for research may be looked up by entering keywords and other metadata in the HDC. This will be further determined in the HDC - work package 6.	The elaboration of these requirements will be coordinated with WP6	EHDS art 57,58
REQ. 1.1	HDAB must assess a data request or health data access application and give permission based on the information provided by the requestor/ applicant and the assessment criteria from the EHDS that a request or application must meet.	Case and Order Management	Completed request/application forms must be distributed to an assessment body (within or by HDAB), the request/application must be assessed, and assessment, results must be returned to the requestor/applicant.	Further details of the assessment procedure will follow in a next phase; T5.2.	EHDS art. 57 (1)(a), art. 67 and 68
REQ. 2.10	HDAB must check whether HDAB permitted research has been published within the period stated following the EHDS.	Case and Order Management	For each research project permitted by HDAB a preliminary title and description of one or more publications must be added within the statutory period, plus the estimated time of publication, also within the statutorily demanded period. Users are obliged to add the actual publication plus link to their research dossier in the HDAB portal and HDAB must flag when no actual publications are registered within the demanded period.	Further details of the publication procedure will follow in a next phase; T5.2.	EHDS art. 57 (1)(a)(iv), art. 61(4) EHDS

REQ. 2.17	HDAB must provide a management system for registering and processing applications and requests and decisions regarding the received requests/applications.	Case and Order management	Management of the registration and processing of applications and requests, as well as the decisions regarding the received requests/applications, including noting responsibilities of different participants in the various stages of the process.	Further details of the assessment procedure will follow at a later stage	EHDS art 57 (1) (e) and (j)
REQ. 2.19	HDAB must provide functionality with which any civilian/patient can inquire about the usage of their personal data. HDAB must publish methods on how data is processed within the HDAB platform and SPE.	Data management & Analytics	The use of every dataset is registered and summarised in published reports. The publication methods of the research for which the data set was used are also documented and published.	This will be further determined in a later stage.	EHDS art. 58 (3)
REQ. 2.20	Depending on how this is implemented in the Netherlands, HDAB may need to provide patients/citizens with the possibility of registering an opt-out. HDAB must manage the removal of data that is associated with a registered opt-out from its catalogue.	Privacy & security	Depending on how this is implemented in the Netherlands, HDAB may need to provide patients/citizens the possibility to register an opt-out or provides a link to that register. HDAB manages the removal of data that is associated with a registered opt-out.	- (Link to) an opt-out registration system; - A process to check data in the catalogue against registered opt-out information.	EHDS art. 71
REQ. 2.21	HDAB must upon receiving an application verify that the applicant satisfies the demands with regard to technical and organisational measures for prevention of misuse.	Case and Order management	HDAB checks if applicants meet EHDS requirements to work with the data applied for.	Further details of the assessment procedure will follow at a later stage	EHDS art 68(1) (d) and (e)

REQ. 2.22	HDAB must, upon receiving an application, verify the identity, authorisation of the applicant as well as their qualifications regarding the use of the requested data and the research that is to be done with that data.	Case and Order management	Upon receipt of application HDAB follows an assessment procedure starting with identification of the applicant	- A checklist against which/with which the identity, authorisation, and qualifications of an applicant can be checked; - A process for the applicant to provide information about identity, authorisation, and qualifications; - A process to check applicants for identity, authorisation, and qualifications.	EHDS art. 67(2)(a), art. 68(1)(d)
REQ. 2.23	HDAB may charge a different fee per data user where this is demanded by national guidelines.	Accounts and Billing	The HDAB determines a fee for each request or application, based on national guidelines.	- A checklist to assess fee amount, based on national guidelines; - A process to facilitate payment of fees; - A process to register payment of fees.	EHDS art 62
REQ. 2.24	HDAB must make requested datasets available to researchers in an SPE within 60 days after receiving the data.	SPE Ordering	HDAB keeps track of date of reception of the data from data holder and date of providing the data to the data user in SPE.	Time stamping of events in DAAMs	EHDS 68(7)
REQ. 2.25	HDAB must inform the data holder of significant findings about individuals whose data has been processed	Data Management & Analytics	HDAB reports significant findings on an individual level to the data holder while ensuring privacy compliance.	A publication results area where summaries and / or links are displayed, in addition to checks whether researchers have fulfilled this duty.	EHDS art. 58 (3) , 61(5)
REQ. 2.26	HDAB is able to forward data requests to a trusted data holder.	Case and Order Management	After issuing a permit to researchers by HDAB their data requests must be transmitted to data holders.	Data requests of researchers with a permit must be transmitted to data holders.	EHDS art. 72(3)

REQ. 2.27	HDAB shall issue or refuse a data permit within 3 months of receiving a complete data access application, with an extension maximum of three months taking into account the urgency and complexity of the request and the volume of requests submitted for decision.	Case and Order Management	HDAB processes applications and ensures that decisions are made within the mandated 3-month timeframe after receiving the application or informs the applicant of any delay.	- A process to track time since application submission; - A process to notify relevant parties if the 3-month timeframe has passed; - A process to communicate about the (passing of the) 3-month timeframe.	EHDS art. 68(4)
REQ. 2.28	Enable logging of formal complaints. HDAB must on its platform provide functionality with which users, data holders, civilians/patients or other third parties can log a formal complaint.	Privacy & Security	HDAB installs a complaint procedure for all types of participants and stakeholders, e.g. users, data holders, civilians/patients or other third parties.	- A platform, process and form to file a complaint; - A process to log and store complaints; - A process to find complaints (both for the submitter and reviewer/processor of the complaint); - A process to respond to complaints.	EHDS art. 81 (1) and (3)
REQ. 2.29	HDAB must, in case of a complaint, provide information on the receipt, processing and resolution of the complaint.	Case and Order Management	HDAB installs a logging and publishing system for all phases and types of complaints.	- A process to log and store complaints; - A process to find complaints (both for the submitter and reviewer/processor of the complaint); - A process to communicate about a complaint (both for the submitter and the reviewer/processor); - A process to respond to complaints.	EHDS art. 81 (1) and (3)
REQ. 2.3	The researcher applying for data access must provide an estimation of the period during which the electronic health data is needed for processing.	Request / Application Management	HDAB provides applicants with a process to provide information about the period of time which they need to process (= do research on) the requested data.	- A process to provide information about the period of time needed for research; - A process to grant access to requested data for the requested period of time;	EHDS art. 67 par 2 sub h

				- A process to revoke access after the requested period of time has passed.	
REQ. 2.4	HDAB must register, as part of the registered health data access applications, a description of the expected results of each research request available.	Request / Application Management	HDAB provides a procedure to provide information about expected results of the research from each application.	A procedure to provide information about the expected results of the research from each data request.	EHDS art. 57 par 1 sub j and art 58 par 1
REQ. 2.41	HDAB must provide a process to request research results (health data request). HDAB shall assess the data request within 3 months. HDAB shall also provide the result of the data request to the requestor within 3 months.	Request / Application Management	HDAB provides a process to request research results. HDAB assesses the request within 3 months. HDAB also provides and publishes the result of the request within 3 months.	- A process, platform and form to request a research result; - A process to log and store research result requests; - A process to respond to/answer research result requests; - A process to communicate about research result requests; - A process to notify relevant parties if the 2-month timeframe has passed.	EHDS 69
REQ. 2.5	HDAB must provide functionality through which the user of the platform is able to see the status of a submitted data request or application.	Request / Application Management	HDAB provides functionality through which the user of the platform is able to see the status of a submitted data request or application.	A process to communicate the status of the submitted data request or application.	EHDS art 57 (1) (e)
REQ. 2.7	HDAB must provide the possibility to apply for two types of requests/applications: information requests (art. 69(2) EHDS) and applications for data research (art 67(2) EHDS)	Request / Application Management	HDAB provides predefined digital forms for both data requests and health data access applications.	The system should enable users to select and complete forms tailored to specific requests, such as requests for information or research. These forms should support dynamic fields so that users can add relevant information,	EHDS art. 67 and art. 69

				with easy storage and validation options.	
REQ. 2.8	HDAB must provide functionality for an accelerated application procedure for specific bodies and reasons (EHDS 68(6)). In that case a decision takes place within two months of receipt, with an extension maximum of one month.	Request / Application Management	HDAB recognises and processes urgent data requests as such when appropriately flagged.	The system must have - a flagging option for urgent requests, - A list of applicable bodies and organisations. - A decision table based upon EHDS 53(1), a-c.	EHDS art. 68(6)
REQ. 3.1	HDAB must keep other HDABs within the HealthData@eu updated of its progress	Governance / Compliance; Privacy & security	Progress updates on HDAB operations should be shared with HealthData@EU stakeholders.	The platform should include a communication module to automatically share periodic progress updates with other HDAB participants within HealthData@EU. This will ensure transparency and collaboration within the European network.	EHDS art 57(1) (i)
REQ. 3.2	HDAB must provide a biennial report on its operations, effectiveness and finances	Data Management & Analytics	The HDAB platform includes a system for generating and distributing (biennial) reports.	Automated reporting tools should capture key metrics of the operations, effectiveness and finances of HDAB. These reports should be available in an easily exportable format for stakeholders.	EHDS art. 59 (1)
REQ. 4.1	The HDAB platform must safeguard the integrity of the use of data through policies that govern: the prevention of any other use of the requested data than the one granted, the protection of the rights of the data holder, and the protection of rights of the patient.	Learning & Assessment	Security mechanisms must enforce strict access and usage policies for datasets.	The system must implement policy-driven security mechanisms to ensure that data is used only for its intended purpose. This includes audit capabilities and protection of the rights of data holders and patients.	EHDS art. 63, art. 52 (3) and (4) and art. 57 (1) c

REQ. 4.10	HDAB must establish that risks for defence, (public) safety and order, and the confidentiality of registration by supervisors, are weighed, either by HDAB or by external expertise (EHDS art. 68 (2)).	Learning & Assessment	Security and confidentiality risks must be assessed and documented as part of HDAB procedures.	Risk assessment workflows should enable assessors to document decisions, with support for external reviews, so that compliance with legal and ethical standards is transparent.	EHDS art. 68 (2)
REQ. 4.11	HDAB must calculate fees according to national and/or European policies.	Accounts and Billing	Fees are calculated in line with the national and/or EU policy principles.	HDAB includes a fee calculation engine that complies with relevant legal and policy guidelines. This allows for accurate fee calculations in accordance with legal requirements.	EHDS art 62
REQ. 4.12	HDAB may charge a fee that is in proportion to the cost of making available electronic health data for secondary use.	Accounts and Billing	Fees for EHDS compliance are calculated and published, covering both the costs of data provisioning and the assessment of requests.	HDAB offers a fee calculator for services, with transparent fee structures and documentation for all users, including a clear explanation of how fees are determined.	EHDS art 62
REQ. 4.13	HDAB will collaborate with the responsible authorities in the Netherlands regarding the implementation and compliance to applicable European and Dutch laws such as DGA, DA, MDR, IVDR, AIA, and the GDPR.	Governance / Compliance	Collaboration frameworks should ensure compliance with national and EU regulations.	HDAB must facilitate regular communication and data exchange with Dutch authorities, including an audit log for legal compliance with the DGA, DA, MDR, IVDR, AIA and GDPR.	EHDS art. 57 (2)(c)
REQ. 4.14	HDAB must comply with the organisational and operations responsibilities stated within the General Administrative Law (Algemene wet bestuursrecht).	Governance / Compliance	Compliance with administrative laws is integrated into HDAB policies and systems.	Workflows should include controls to ensure that all actions comply with the General Administrative Law Act. This includes built-in notifications to flag potential violations and automatic reporting for full transparency.	Awb

REQ. 4.16	The protection of rights of the patient regarding data usage.	SPE Ordering	HDAB manages usage agreements with regard to time limitations for data usage and storage. These agreements are shared with the applicant during the ordering process, and compliance is monitored throughout the provision phase.	Agreement Provisioning: - The system must include a standardized clause, in compliance with the EHDS, in all data usage agreements specifying the allowed time for data usage and storage within the SPE. Configuration of time limits: - Administrators must have the ability to configure time limits for data usage and storage on a per-agreement basis. Automated Notifications: - The system must send reminders to data requestors when the data usage/storage period is nearing its end. Compliance Monitoring: - Ensure periodic audits are conducted to verify that data usage and storage adhere to the agreed time limits. Agreement Accessibility: - - - Provide a digital copy of the data usage agreement, including time restrictions, to the data requestor via the portal. Allow requestors to review agreement terms as part of the SPE ordering and provisioning process.	EHDS 68, 69

REQ. 4.17	HDAB must involve and inform stakeholders regarding the definition and execution of its business strategy to ensure alignment of the needs of the stakeholders with the goals of the HDAB organisation.	Governance / Compliance	HDAB facilitates structured engagement with stakeholders by organising consultations, sharing strategic plans, and gathering feedback. This ensures that stakeholder needs are identified and aligned with the organisation's objectives, fostering transparency and trust.	Establish a formal process to engage stakeholders through forums, workshops, or meetings and share strategic documents and updates via a dedicated platform. A mechanism must be implemented to collect feedback and integrate it into strategy revisions, ensuring alignment with stakeholder needs. Compliance must be maintained by documenting interactions and decisions, with an audit trail for governance. Regular progress updates and reports, including KPIs, must be provided to monitor and demonstrate the alignment of organisational goals with stakeholder contributions.	EHDS art. 55 par 4 and art. 57 (2)(b)
REQ. 4.18	HDAB must publish guidelines and policy defining acceptable use of the platform and SPE, as well as measures to prevent unfair use of data or misuse of the facilities HDAB offers.	Governance / Compliance	HDAB ensures transparency and accountability by providing clear guidelines and policies for all users of the HDAB platform and SPE. These documents define acceptable use, outline measures to prevent unfair data practices, and establish protocols to detect and address potential misuse.	HDAB must develop and publish comprehensive guidelines and policies that define acceptable use of the platform and SPE, including measures to prevent unfair data practices or misuse of facilities. These documents must be accessible to all stakeholders and include specific provisions for monitoring compliance and addressing violations. The system must support automated notifications for policy updates, offer a mechanism for	EHDS art 73(5)

				reporting misuse, and maintain an audit trail of actions.	
REQ. 4.19	HDAB must (be allowed to) take decisions on applications with purposes for secondary use as defined by the EHDS, within 3 months of receipt, up to 3-month extension possible.	Request / Application Management	HDAB processes applications and ensures that decisions are made within the mandated 3-month timeframe, with a possible 3-month extension under justified circumstances.	HDAB must implement a tracking system to monitor the decision timeline for applications. Notifications must be sent to stakeholders when an application is received, during the decision-making process, and upon any extensions. The system must allow administrators to document reasons for extensions and ensure decisions are finalised and communicated within the allowable period. A dashboard must display the status of all applications, highlighting pending deadlines to prevent delays and ensure compliance.	EHDS 68.4, 68.6
REQ. 4.2	The HDAB must ensure transparency by publicly sharing descriptive information on all submitted data requests and applications, including their state, assessment, and results	Data Management & Analytics	HDAB shares publicly detailed information on all submitted data requests and applications, including their status, assessment outcomes, and results.	HDAB must develop a publicly accessible platform to provide insights into the number, type, and outcomes of requests. The system must ensure that published data is in compliance with the EHDS.	EHDS art. 57 (1) (j)
REQ. 4.20	HDAB shall assess if the health data request is complete and take into account the risks referred to in Article 69(2). HDAB shall assess the health data request within three months of receipt of the request and, where possible,	Governance / Compliance	HDAB ensures compliance with regulatory timelines by evaluating and deciding on requests with purposes for secondary use as defined in the EHDS (article 53(1). HDAB shall also provide the	HDAB must implement a system to monitor the 3-month decision timeline for requests with purposes for secondary use as defined in the EHDS, and the propagation of the response. The system must maintain an audit trail	EHDS art 69(2), 69(4)

	subsequently provide the response to the health data user within a further three months		response within the regulatory period. Decisions are documented and communicated to ensure accountability and transparency.	of decisions, extensions, and communications.	
REQ. 4.21	HDAB must assess requests and applications based on the ethical use of the data and the purpose of the request or application based on guidelines provided within Dutch law. This includes assessment of a request or application when a patient opt-out cannot be honoured.	Governance / Compliance	HDAB evaluates requests and applications to ensure these align with ethical standards and the legal framework. Requests and applications involving exceptions to patient opt-outs are reviewed to justify and document compliance with Dutch law and ethical principles.	HDAB must establish a review system to evaluate the ethical use and purpose of data requests in accordance with Dutch legal guidelines. The system must enable detailed assessment of requests invoking exceptions to patient opt-outs, including documentation of the rationale and legal basis for such exceptions.	EHDS art. 71 par 4 jo art. 68 par. 1 under g
REQ. 4.22	HDAB must facilitate research on data from other (EER) countries when a request for this data is incorporated in a licensed application.	Request / Application Management	The HDAB enables cross-border research by incorporating data requests from other EER countries into licensed applications. Other data (from EER countries) than only catalogue data can be added to a research request.	HDAB must provide a mechanism to integrate and process data requests from other EER countries as part of licensed applications. The system must support secure data exchange, ensure compliance with EER regulations, and document the licensing process for cross-border requests. Notifications must be sent to the applicant regarding the status and approval of EER data integration.	EHDS 75
REQ. 4.4	HDAB must establish policies for the quality and state of the datasets the data holders intend to publish in the Health Data Catalogue (HDC), regarding data	Governance / Compliance	HDAB stipulates policies and good practices that datasets published in the HDC meet defined quality and	HDAB must define and publish policies outlining criteria for dataset quality, privacy protection, data minimisation, and completeness. It should enforce the	EHDS art 66, 77-80

	quality, privacy, data minimisation, completeness and a minimum set of meta data.		security standards by implementing clear policies.	inclusion of a mandatory minimum set of meta data for each dataset and provide templates or guidelines to assist data holders.	
REQ. 4.5	The HDAB must share information regarding the usage of the platform with all active stakeholders (EHDS 59 (1a))	Learning & Assessment	HDAB fosters transparency and continuous improvement by sharing insights and usage statistics of the platform with active stakeholders.	The system must provide a platform that supports notifications for periodic updates or significant changes in usage trends. Additionally, training materials or knowledge-sharing sessions must be provided to help stakeholders interpret and leverage these insights effectively.	EHDS 59 (1a)
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).	Governance / Compliance	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)
REQ. 4.8	HDAB ensures transparency by publishing clear policies on the required licenses and approvals for accessing and using its services.	Governance / Compliance	HDAB ensures transparency by publishing clear policies on the required licenses and approvals for accessing and using its services.	The system must provide an easily accessible platform where the HDAB policies regarding licenses and approvals are published and regularly updated. These policies should include detailed information on the licensing requirements, application procedures,	EHDS art. 57 par 1 sub j.

				and any necessary approvals to use HDAB services. The platform should allow stakeholders to download and review these policies and provide a mechanism for stakeholders to request further clarification. Notifications should alert users to any changes in the policies or licensing requirements.	
REQ. 5.1	HDAB must provide an overview of the system requirements and security prerequisites that allow the configuration of an SPE and provision of access to verified users.	SPE Ordering	In DAAMs, the requirements and wishes of the data user for an SPE may be specified, within the boundaries of the EHDS requirements, and the access rights for the user may be regulated.	The application form must also include the possibilities for directing to an SPE or configuration of an SPE. The requested design wishes/requirements must be in accordance with EHDS requirements and be passed on to the process of the SPE design.	EHDS 55
REQ. 5.2	The HDAB system needs to, as part of the application process, facilitate functionality where the applicant describes the limited purpose of the data that is requested.	Request / Application Management	Within the DAAMs system, the applicant must be able to indicate the reasons for the requested data (purpose of the research/basis).	The application form must contain fields where the purpose of each requested dataset within the research can be indicated.	67(2) bcd
REQ. 5.3	HDAB must keep an audit trail of all health data access applications and usage of datasets as well as all activities within the HDAB environment. This must include (all) user actions and data manipulation activities done within the SPE. (in consideration 68, art 73(3), indirect art 59 (1)(c) and (d) EHDS)	Data Management & Analytics	HDAB keeps track of which applications are submitted, and which data processing activities take place around and within the SP.	HDAB must log the requests via DAAMs in their various phases. HDAB must also record who has access to SPE where and what data is coming in and going out.	in consideration 68, art 73(3), indirect art 59 (1)(c) and (d) EHDS

REQ. 5.4	Any fees charged to health data users by the health data access bodies or health data holders (EHDS art. 62) shall be transparent and non-discriminatory. (EHDS art 62(3))	Accounts and Billing	Organising payments to data users and compensation to data holders. Data usage fees are transparent during the application process.	Automate payments and invoicing; set up transparent invoicing.	EHDS art 62(3)
REQ. 6.1	HDAB must ensure that there is sufficient capacity both in personnel and finances to support the management tasks HDAB is obligated to cover.	Platform Management	Management of the HDAB facilities (personnel, finances). For DAAMS, this specifically involves ensuring the technical and organisational sustainability of the system.	This will be determined in a later stage.	EHDS 55(2)
REQ. 7.1	HDAB is obligated to forward any complaints about the unfair use of data or the leaking of personal information directly with the Dutch DPA (Autoriteit Persoonsgegevens).	Privacy & Security	HDAB organises that risk issues and complaints are registered and distributed to the Dutch DPA (Autoriteit Persoonsgegevens).	Setting up communication with Dutch DPA (Autoriteit Persoonsgegevens; AP) and rules for this.	EHDS 81(4)
REQ. 7.6	HDAB must provide a Secure Processing Environment (SPE) in which the researcher can execute his/her research on the requested datasets	SPE Ordering	The provision of an SPE by HDAB.	Indicate available SPEs in DAAMS with their capabilities and costs.	EHDS art 73
REQ. 7.7	HDAB must implement protective measures under the DGA Implementing Act for non-personal health data made available to a user outside EU jurisdiction and must take all reasonable technical, legal and organisational measures to prevent transfers of non-personal health data outside EU jurisdiction where this	Governance / Compliance; Privacy & Security	Organising rules and security systems around the use of data by non-EU users and transfer to non-EU territory.	Identifying non-EU data users, controlling the use of non-personal health data by non-EU data users, controlling the transfer of non-personal health data to non-EU countries.	EHDS art. 88

	would conflict with national or European Union law.				

Health
Data Access
Body-NL

Denk mee. Praat mee. Bouw mee.