D6.3 Guideline for Health Data Access Bodies on the procedures and formats for data access

TEHDAS2 – Second Joint Action Towards the European Health Data Space

17 September 2025

Co-funded by the European Union

0 Document info

Disclaimer

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HaDEA. Neither the European Union nor the granting authority can be held responsible for them.

0.1 Authors

Authors	Organisation
Rosa Juuti	Finnish Social and Health Data Permit Authority Findata, Finland (Lead organisation)
Asimina Boubaki	Ministry of Health, Greece
Markus Helfert	Maynooth University, Ireland
Denise Manton	Maynooth University, Ireland
Dzintars Mozgis	Centre for Disease Prevention and Control of Latvia
Inka Närhi	Finnish Social and Health Data Permit Authority Findata, Finland (Lead organisation)
Nicoletta Prentzas	CYENS, Cyprus
Sonja Saloranta West	Finnish Social and Health Data Permit Authority Findata, Finland (Lead organisation)
Sam Santosh	Maynooth University, Ireland
Aurēlija Usačova	Centre for Disease Prevention and Control of Latvia
Eva Zvirgzdiņa	Centre for Disease Prevention and Control of Latvia

0.2 Keywords

Keywords	TEHDAS2, Joint Action, Health Data, Health Data Space

0.3 Document history

Date	Version	Editor	Change	Status
December 2024	0.1	Inka Närhi, Rosa Juuti contributors	First draft	Draft
December 2024	0.2	Inka Närhi	Second draft, comments adapted	Draft
January-March 2025	1.0	Major contributors + Rosa Juuti	Development of subsections	Draft
April 2025		Commenting by task 6.3 team, DG SANTÉ		

Date	Version	Editor	Change	Status
		team and collaborators from tasks 7.2 and 6.1		
May 2025	1.2	Major contributors + Rosa Juuti	Updates according to the received comments	Draft
June 2025	1.3	Rosa Juuti and Sonja Saloranta West	Harmonisation and finalisation of the draft	Draft
July-August 2025	1.4	TEHDAS2 participants, DG SANTÉ	TEHDAS2 internal commenting round for all wave 2 deliverable drafts	Pre-final
August-September 2025	1.5	Rosa Juuti and Sonja Saloranta West	Updates according to internal TEHDAS2 review, DG SANTÉ team and PSG	Final draft
			New version based on public consultation feedback	

Accepted in Project Steering Group on 11 September 2025.

Contents

1 Abbreviations

Abbreviation	Description
Art	Article
DAAMS	Data Access Application Management System
EEA	European Economic Area
EHDS	European Health Data Space
EU	European Union
GDPR	General Data Protection Regulation
HDAB	Health Data Access Body
IPR	Intellectual Property Rights
SPE	Secure Processing Environment
TEHDAS2	Second Joint Action Towards the European Health Data Space
TS	Trade Secret
UHDAS	Union Health Data Access Service
VAT	Value-Added Tax

2 Executive summary

In the scope of TEHDAS2 (the second joint action Towards the European Health Data Space), this guideline elaborates in detail the different processes that health data access bodies (HDABs) go through in order to implement their responsibilities under Articles 67–69, 72 and 73 of the European Health Data Space (EHDS) regulation: to manage and assess health data access applications and health data requests, to issue data permits and approve health data requests, to obtain data from health data holders, to interact with trusted health data holders, to cooperate with health data users and to enable data access to facilitate the secondary use of health data.

As such, the guideline focuses on three distinct stages in the workflow: the necessary application completeness checks that are followed by the thorough assessment and evaluation of the applications and requests. Subsequently, the guideline describes what takes place after a data permit has been granted or a data request approved.

Checking the completeness of data access applications and data requests is the necessary first step to verify that all required information is provided for and is filled out properly, without prejudging the legal admissibility or scientific validity of the application. The checks described in this guideline aim to ensure technical completeness, semantically valid input and contextual consistency of the application. The proposed checks differ based on whether the HDAB is handling a health data access application or a health data request.

Following the application completeness check, the assessment process - to decide whether a data permit should be issued, or a health data request approved - is comprehensively described. This guideline focuses on ensuring that all necessary requirements for information included in an application deemed complete are met according to the provisions of the EHDS regulation. During the assessment of the application, and for the purposes of issuing a data permit or approving a data request, this guideline emphasises the fulfilment of the specific criteria that are outlined in the EHDS regulation. It should be noted that the suggested framework allows member states to define and operationalise their own specific processes, provided they remain within the boundaries of the EHDS regulation. A concise overview of the procedural time frame is also provided in the document.

Finally, the guideline briefly describes the actions undertaken by the HDAB that follow the decision, in coordination with health data holders and health data users. The decision is either a data permit, a data request approval, or a refusal. The guideline outlines the coordination of secure data extraction and transmission, the data preparation, making data available in secure processing environments (SPEs) and communicating with the SPEs. Additionally, the guideline also provides basic information of administrative processes such as invoicing for the provided services, the continuous monitoring of compliance and documentation processes. Especially the actions to be taken after the decision are largely in the scope of other TEHDAS2 documents and in such cases the relevant document is referred to.

This guideline serves as operational guidance for HDABs describing all the procedural steps from receiving an application, to issuing a decision, to actions to be conducted after the approval. In doing so, it ensures alignment with both the EHDS regulation and the General Data Protection Regulation (GDPR).

3 Introduction

Advancing health data use in the European Health Union

As part of the European Health Union, the European Union (EU) is advancing the use of health data for secondary purposes, including research, innovation and policymaking. Smooth and secure access to data will drive the development of new treatments and medicines and optimise resource utilisation—all with the overarching goal of improving the health of citizens across Europe.

TEHDAS2, the second joint action Towards the European Health Data Space, represents a significant step forward in this vision. The project will develop guidelines and technical specifications to facilitate smooth cross-border use of health data and support health data holders, health data users and the new health data access bodies in fulfilling their responsibilities and obligations outlined in the EHDS regulation.

TEHDAS2 focuses on several critical aspects of health data use.

- Data discovery: findability and availability of health data, ensuring it is accessible for secondary purposes.
- Data access: developing harmonised access procedures and establishing standardised approaches for granting data access across member states.
- Secure processing environment: defining technical specifications for environments where sensitive health data can be processed safely.
- Citizen-centric obligations: providing guidance on fulfilling obligations to citizens, such as communicating significant research findings that impact their health, informing them about research outcomes and ensuring transparency in how their data are used.
- Collaboration models: developing guidance on collaboration and guidelines on fees and penalties as well as third country and international access to data.

TEHDAS2 will contribute to harmonised implementation of the EHDS regulation through the concrete guidelines and technical specifications. Some of these documents and resources will also provide input to implementing acts of the regulation. Hence, the joint action will increase the preparedness for the EHDS implementation and lead to better coordination of member states' joint efforts towards the secondary use of health data, while also reducing fragmentation in policies and practices related to secondary use.

The EHDS regulation and health data access bodies

Secondary use of electronic health data can bring great benefits, but it is important that datasets are accessible, of high quality and suitable for the purpose of creating scientific, innovative and societal value, whilst at the same time all the necessary safeguards are in place to ensure data protection, safety, confidentiality and mitigation of risks.

Without hindering or replacing existing mechanisms or contractual agreements, the EHDS regulation establishes a common framework to access electronic health data for secondary use and for the purposes defined in the regulation. Under this framework, health data holders should make the data they hold available based on a data permit or a health data request approval. To operationalise the requirements, one or more HDABs shall be appointed in each member state, data processing shall

take place in an SPE (in the case of a data permit) and requirements for proper data processing shall be set out in the data permits and data request approvals.

Therefore, the main responsibilities of an HDAB in the scope of this guideline, according to Article 57 of the EHDS regulation, include:

- deciding on health data access applications pursuant to Article 67 of the regulation, authorising and issuing data permits pursuant to Article 68 to access electronic health data and deciding on health data requests pursuant to Article 69, also in accordance with Chapter II of Regulation (EU) 2022/868,
- maintaining a management system to record and process health data access applications, health data requests, data permits issued and health data requests approved
- publishing metadata catalogues on the source and nature of electronic health data available at national level, in accordance with Articles 77, 78 and 80,
- 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,
- receiving, combining, preparing and compiling the requested datasets as defined in the granted permit or request and ensuring that anonymisation or pseudonymisation measures are applied as appropriate,
- preserving 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,
- providing access to electronic health data to health data users pursuant to a data permit in a secure processing environment (SPE) in accordance with Article 73,
- maintaining and managing public information systems to record the handling of health data applications and requests as well as measures related to non-compliance pursuant to Article 63, to publish the results communicated by health data users pursuant to Article 61(4) and to inform the citizens on the conditions under which data are made available and on how their rights are protected and safeguarded according to Article 58,
- monitoring and supervising compliance of health data users and health data holders with the requirements laid down in the regulation and coordinating with supervisory authorities where necessary,
- 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.

3.1 Target audience

The guideline is intended for the following audiences:

HDABs: To provide practical guidance for implementing their responsibilities under Articles 67–69, 72 and 73 of the EHDS Regulation, including on how to check application completeness, assess applications and requests, issue permits and perform required actions after the decision.

Health data applicants (e.g. researchers, public authorities): To explain how different aspects of the applications are reviewed and assessed and what to expect from the HDAB review process.

Health data holders and trusted health data holders: To clarify their role during the application assessment process. For trusted data holders specifically, the guideline outlines expectations when assessing applications under Article 72.

Public sector institutions and EU bodies: To support and clarify their dual role as potential health data applicants or health data holders under the EHDS framework.

3.2 Purpose

The purpose of this document is to support the harmonised implementation of the EHDS regulation across member states, proposing a consistent way of handling data access applications or data requests, issuing data permits or data request approvals and enabling the secondary use of health data.

More specifically, the document provides guidelines on the procedures involved in the entire lifecycle of secondary use of health data - starting with the completeness checks of submitted data access applications or health data requests by health data applicants, to a consistent and methodological approach for their assessment process. This includes validating that health data applicants have only applied for data that are adequate, relevant and limited to what is necessary in relation to the declared purpose of use. The guideline will both introduce mandatory tasks of the HDAB according to the EHDS regulation, as well as provide practical suggestions.

In addition, the actions following approval are also addressed, including data extraction, data sharing, monitoring of compliance and publication of research outputs. In most cases, the described actions following approval are covered more in depth in other TEHDAS2 documents and in these cases the relevant document is appropriately referred to.

Please note that this guideline and especially its chapters 5 and 6 about application completeness check and assessment, should be read together with the application forms (templates in annexes 5 and 6). These chapters of the guideline act as a handbook for application processing and they are not fully self-explanatory.

This guidance and the annexed templates are non-binding and may be updated as further implementing acts and delegated acts are adopted by the European Commission, or guidelines by the EHDS Board (see e.g. Article 70 in the EHDS regulation regarding templates).

4 Scope

This guideline is part of a series developed under TEHDAS2 project to operationalise the EHDS regulation, specifically addressing Chapter IV on secondary use of health data. The scope of this guideline begins after the data discovery phase, once the applicant has identified the datasets of interest in the EU or national dataset catalogue and has submitted a health data access application or a health data request via the central platform or HDAB's own application system. This guideline is based on the templates for the data access application, data request and data permit that are available in the HealthData@EU Central Platform. These templates are annexed to this guideline as annexes (annexes 5, 6 and 9, respectively). In this guideline, the term "application" refers to both health data access applications and health data requests. When the guideline refers to only one of these, it is clearly stated.

This guideline focuses on the role of the HDAB and provides an overview of the entire workflow in the data access application and the data request journey. It focuses on the operational processes required to enable health data sharing according to Chapter IV of the EHDS regulation – from the issuance of data permits and data request approvals to the data processing through SPEs once a permit has been granted. Where applicable, this guideline and recommended procedures also apply to trusted health data holders, when they are fulfilling their duties under Article 72 and to the European Commission's Union Health Data Access Service (UHDAS), when the health data holders are EU institutions, bodies, offices or agencies in line with Article 56. Overall, the document serves as the operational interpretation of Articles 67 to 69, 72 and 73, providing guidance to support the EHDS implementation.

As already mentioned, the guideline recommends that a completeness check on the information provided in the data access applications or health data requests should precede the assessment of the necessary criteria to grant a permit or approve a request. The completeness check serves as a pre-screening test that verifies that all mandatory information has been submitted successfully: it is either uploaded as an attachment, in the format of free text or as selection from check lists. This cannot be done entirely automatically. The completeness check is a formal validation step - not a substantive review - and must not include judgements on content adequacy or project quality. This distinction is essential for legal clarity and efficiency. Both processes, the completeness check and the assessment that leads either to a refusal or to a data permit / data request approval, are outlined and operationalised in detail, with proper references to the relevant EHDS provisions.

Finally, the guideline lists the post-approval processes that involve for example data extraction and secure, transparent and appropriate data sharing, continuous compliance monitoring mechanisms, administrative mechanisms and dissemination of outcomes.

5 Application completeness check

The completeness check ensures that an application is complete (Articles 68(4) and 69(3)). This step is not meant to assess the quality or scientific value of the application, but only to verify that required fields are filled with plausible content, enabling the application to move forward to the actual assessment phase. Only complete applications shall be taken to processing. Performing of this check must not lead to undue delays in line with the limits defined in Article 68(4) of the EHDS regulation and further discussed in Chapter 8 of this document.

Although the completeness check and the opportunity to complete an incomplete application is not explicitly foreseen in the EHDS regulation for health data requests, there is no prohibition either. It is therefore possible and advisable to check a health data request for its completeness before the application assessment phase.

Application form templates are attached to this guideline: Annex 5 for health data access application and Annex 6 for health data request, respectively.

Please see Annexes 7 and 8 for checklists for checking the health data access application and health data request, respectively, that can be used as helpful tools for the completeness checks.

Please see Chapter 8 for information on time frames.

5.1 Making applications public

The EHDS regulation mandates that the HDAB shall make public, through electronic means, any health data access application and health data request without undue delay after initial reception [Article 57(1)(j)(ii)]. The publication should occur as soon as possible after the application is received, even if it is later found to be incomplete and requiring amendments. This means that the publication takes place prior to the completeness check.

Updated versions or changes to the application introduced later during the completeness check and assessment phases can be published as updates to the same entry.

The purpose of publishing applications is to provide transparency. The HDAB must be aware that applications can contain e.g. contact information, banking details, trade secrets and information under intellectual property rights (IPR). Therefore, the HDAB can consider to not publish the application in full, but rather certain sections of it. If the whole application is not published, the HDAB needs to be able to justify any omissions.

5.2 Defining a ‘complete application’ ready for processing

In the EHDS regulation, a ‘complete application’ is not defined. Completeness aims for a minimum level of information provided in the application. A ‘complete application’ is one where all required information is provided, and it is also contextually relevant and semantically meaningful. Semantically meaningful means that input fields are expected to contain recognisable text, meaningful response and logically appropriate values. Contextual relevance can ensure that related fields align correctly, and the provided information is coherent.

Following the definition of a ‘complete application’, the following types of completeness checks can be defined:

(i) technical completeness: all mandatory fields are filled in and attachments can be opened, are not empty or clearly incomplete. As mentioned above, the DAAMs will ensure the first one, but the latter should be checked by the HDAB personnel.

(ii) semantically meaningful/valid (does the input make sense?): text fields (e.g. project name) contain real words (not random characters), numerical fields (e.g. phone number) contain valid values, address fields contain text that resembles a real address format, etc.

(iii) contextual consistency (is the input relevant?): ensure that the provided text fits within the expected content, cross-field consistency. This check is aimed to identifying illogical or contradictory issues in the application, not to evaluate e.g. the project rationale for being scientifically sound.

The checks for semantic validity and contextual consistency should be understood as sanity checks (e.g. detecting clearly nonsensical entries or missing attachments) and not as in-depth assessment of relevance or sufficiency, which is outside the scope of this phase.

The completeness check step helps the HDAB verify that each application is complete and filled out properly. The aim is to make sure that the HDAB has all the necessary information to process the application and avoid losing time with processing incomplete applications.

5.3 Completeness check steps

Data Access Application Management systems (DAAMs) shall ensure that every mandatory field of the application is filled in before it can be submitted. For multi-country applications the HealthData@EU Central Platform will manage this. Format checks and semi-automated validations would be desirable, but further developments of the HealthData@EU central platform and national DAAMs are needed. Where feasible, the national systems of the member states can introduce automated plausibility controls for selected fields. For example, the following fields are potential candidates for automated validation (IBAN, VAT number, Operator ID, Business ID) as they follow known national or European formatting rules.

However, the substantive quality or relevance of the information provided cannot be assessed automatically. Hence, the completeness check step is recommended to ensure completeness in terms of plausibility of values in the input fields – that the application is complete for processing. It should be verified that the necessary information is provided and is relevant for the application specifics, in accordance with Article 67 (2) and Article 69 (2) for health data access applications and health data requests, respectively.

It is advisable to scan through all mandatory fields from the common data access application form or common data request form, as in the HealthData@EU central platform implementation. Under the assumption that these forms ensure the submission of a technically complete data access application or data request, completeness check can focus on the (ii) and (iii) types of checks as described above in chapter 5.2, in addition to checking the attachments. Common plausibility completeness checks are presented in Table 1 below.

Under the assumption that the completeness check will take place online, via the application form, mandatory fields can be scanned section by section.

Table 1. Common plausibility completeness checks.

Field / information	Check
Natural person name	Resembles a real person's name – no random characters (e.g. fd3fd3) or fake names, one or more words in a typical human name format expected.
Legal entity name Affiliation	Resemble an organisation name – no random characters or placeholders, full / official business name expected (e.g. Medical Research Centre).
Email	Resembles a real email address - flag obvious invalid entries like name@mail.com, test@test.com.
Phone	Resembles a real phone number - flag obvious invalid entries like repetitive numbers
Job title	Resembles a common industry role
Address	Resembles a postal address
Attachment	File is not corrupted and not empty. The File type matches to an item on a list of allowed file types of the common application forms: pdf, doc, docx, xls, xlsx and odt file types. Maximum file size is 5 MB

Notes on language

The EHDS regulation does not impose any specific language regimes for data access applications or data requests.

For the multi-country applications, the design of the HealthData@EU Central Platform ensures that applications can be submitted in any official EU language. Once submitted, the application is automatically translated and transmitted to the relevant HDAB(s) in 1) the original language in which the application was submitted; 2) English; 3) the official language(s) of the member state the HDAB is located in; and 4) in the national languages of all the member states whose data the application concerns.

For applications that concern only data from one member state, the HDAB(s) may define in their national procedures in which official EU languages applications are accepted, in accordance with national language legislation and their administrative capacity. It is recommended that at minimum the HDABs would accept applications in their national language(s) and English to support accessibility.

Notes on application sections

The HDAB can receive:

- Health data access applications, for access to anonymised or pseudonymised individual-level electronic health data within an SPE, and

- Health data requests, for access to anonymised, aggregated (non-individual-level) statistics.

Table 2 describes which sections of the common application forms shall be assessed per application type. The application forms are included as annexes of this guideline: Annex 5 for data access application and Annex 6 for data request, respectively.

Table 2. Sections of the common application form to be reviewed per application type.

Section of the common application form	Included in the data access application	Included in the data request
1. Selecting data sources for the project	Yes	Yes
2. Public information of the project	Yes	Yes
3. Applicant and contact person information	Yes	Yes
4. Payment details	Yes	Yes
5. Purpose of data use	Yes	Yes
6. Description of the data needed	Yes	Yes
6.1. Defining the extraction criteria for the cohort	Yes	Yes
• Questions related to the compilation of statistics	No	Yes
6.2. Defining the extraction criteria for the controls	Yes (*if applicable*)	No
6.3. Defining the extraction criteria for relatives	Yes (*if applicable*)	No
7. Other data to be combined	Yes	No
8. Data processing, data protection and safeguards to prevent unauthorized use of data	Yes	No
9. Additional information	Yes	Yes
10. Confirmation of information	Yes	Yes

In conclusion, the instructions for completeness check and assessment are identical for data access applications and data requests, apart from sections 6, 7 and 8, which have separate instructions for different application types.

Section 1 is not formally part of the common application forms as it includes the selection of the data sets from the EU Dataset Catalogue that will be applied for. Section 9 includes only two voluntary fields related to additional information and Section 10 includes three points that the health data applicant must agree on before submitting the application. These sections are not further discussed in this guideline.

5.4 How to check the completeness of applications

Before scanning the application fields, the following should be checked:

- Verify that the application has been submitted to the correct HDAB.
- If similar health data request and health data access applications are submitted

- The HDAB should ask the applicant to clarify the intended path, without trying to interpret the project's scientific goals at this stage.
- Clarify with the applicant if both applications or only one of them should be processed.
- Similarity can be assessed e.g. by comparing the applicant, data sources, the purpose(s) for which the data will be used and name of the project.
- Health data access application and health data request -specific completeness checks are presented in detail below, section by section (Chapters 5.4.1 and 5.4.2, respectively).

Note to the reader: The following sections can be checked in a similar fashion for both data access applications and data requests. The numbering refers to the numbering of the sections in the common application forms.

Section 2 – Public information of the project

The applicant provides a general overview of the project that is fit for public disclosure which contributes to fulfilling transparency requirements under Articles 58 and 61(4) of the EHDS Regulation. Check the following:

- Project name: appears to be a plausible project title (i.e. not a placeholder or random characters).
- Project leader name: see 'Common plausibility checks' (Table 1; natural person name or legal entity name).
- Description of the data the applicant will use: it should be consistent with the project sources selected (e.g. sources match declared purpose) – a basic coherence check, not an in-depth analysis.
- Summary of the project: the description should be consistent with the selected research objectives, areas of research and the project sources.

Section 3 – Applicant and contact person information

The applicant provides detailed information about the applicant and the primary contact person. Check the following by screening for clearly impossible or missing entries (there is no need to confirm organisational affiliations or legal status at this stage):

- Applicant name: an applicant could be a legal or a natural person: see 'Common plausibility checks' (Table 1; natural person name or legal entity name)
- Postal address (street and number, zip code, city/town, country): see 'Common plausibility checks' Table (Table 1; address)
- If the applicant is a natural person, they also need to provide the following:
  - Email: see 'Common plausibility checks' (Table 1; email)
  - Phone: see 'Common plausibility checks' (Table 1; phone)
  - Job title: see 'Common plausibility checks' (Table 1; job title)

- Affiliation: see ‘Common plausibility checks’ (Table 1; legal person name)

- If the applicant is a Legal person, they need to provide Contact person information:
  - Full name of the contact person: see ‘Common plausibility checks’ (Table 1; natural person name)
  - Email: see ‘Common plausibility checks’ (Table 1; email)
  - Phone: see ‘Common plausibility checks’ (Table 1; phone)
  - Name of the organisation: see ‘Common plausibility checks’ (Table 1; legal person name)
  - Business ID of the organisation: consists of characters and/or numbers (e.g. OP123456)
  - Job title: see ‘Common plausibility checks’ (Table 1; Job title)
  - Affiliation: see ‘Common plausibility checks’ (Table 1; legal person name)
  - Contact person and applicant relationship: should indicate a reasonable link (e.g. employee, consultant) between the natural person and the legal entity.)

Section 4 – Payment details

The applicant provides information on payment details of the person and/or organisation to whom the HDAB addresses the bills related to the application. Check the following:

- Full Name: see ‘Common plausibility checks’ (Table 1; natural person name)
- Postal Address: see ‘Common plausibility checks’ (Table 1; address)
- Phone Number: see ‘Common plausibility checks’ (Table 1; phone)
- Email: see ‘Common plausibility checks’ (Table 1; email)
- Invoice Reference Number: consists of characters and/or numbers (e.g. 789XYZ123)
- E-invoice banking Address (IBAN): consists of characters and/or numbers
- Operator ID: consists of characters and/or numbers (e.g. OP123456)
- Name of the Organisation: see ‘Common plausibility checks’ (Table 1; legal person name)
- Business ID of the Organisation: consists of characters and/or numbers
- Value-added tax (VAT) Number: consists of characters and/or numbers (e.g. FI9876543210)

Section 5 – Purpose of data use

The applicant provides information about the person responsible for the data use, the person responsible for the research and other information related to the purposes of data use selected in Section 2. The applicant fills in the required fields according to the selected purposes of data use.

Check the following (if applicable):

- For Person-related fields (person responsible for data use or person responsible for the research):
    - Full name: see Common plausibility checks' (Table 1; natural person name)
    - Job title: see Common plausibility checks' (Table 1; job title)
    - Affiliation: see Common plausibility checks' (Table 1; legal person name)
- The applicant provided an answer (not just random text) to the question "Why are the data the applicant is applying for needed for the indicated purpose of use?"
- The applicant provided an answer (not just random text) to the question "What is the aim and topic of your project?"
- The applicant provided an answer (not just random text) to the question "Which are the expected benefits related to the use of the electronic health data and how this benefit contributes to the purposes referred to in 5.1?".
- The applicant attached a summary of the plan for using the data. The uploaded file can be opened, is readable and is not empty.
- The applicant attached a summary of the research plan. The uploaded file can be opened, is readable and is not empty.

Legal basis: (applicable if the applicant has chosen "Policy making and regulatory activities to support public sector bodies or Union institutions, bodies, offices and agencies, including regulatory authorities, in the health or care sector to carry out their tasks defined in their mandates" as the purpose of use

- The applicant specified the legal basis, for example the relevant legislation, which assigns a task falling within the applicant's mandate and confirms that the applicant's planned use of the data is to facilitate such tasks.
- The applicant provided a link to the supporting documentation as evidence of the legal basis, it should not be a broken link. This could be e.g. a link to applicable legislation or an official document declaring the legal basis.

At this stage, you should only check that a legal basis is declared and that the link or file is present and functional – not whether it is legally sound and admissible.

5.4.1 Data access application -specific checks

Note to the reader: In addition to the checks of Chapter 5.4, the completeness check of data access applications should include the following checks, specific for data access applications.

Section 6 – Description of the data needed

The applicant provides a description of the required data for each country/HDAB included in their application. Many of the fields regarding the selected data sets will be prefilled based on the data sources the applicant has selected from the EU Dataset Catalogue prior to opening the application form. Section 6 input fields are organised into four subsections. Check the following:

Subsection 6 – Description of the data needed

- The applicant provided an answer (not just random text) to the question about the data linkage plan. The plan should describe how the data from various resources will be linked together, e.g. based on a personal identification code or through subject similarity metrics. At this point you should only check that a response to the question is given, not to assess if the chosen method is likely to result in unique matches.

Subsection 6.1 – Defining the extraction criteria for the study cohort

- The applicant defines how the study cohort is formed and answers a set of questions based on the option selected. The study cohort can be established using:
  - (i) criteria from the application form,
  - (ii) a previously established cohort,
  - (iii) a combination of options (i) and (ii),
  - (iv) the entire population of a country, state or other area.
- The applicant explained whether data subjects have been informed about the planned data use and if not, described the transparency measures they will implement. (study cohort options (i), (iii), (iv)).
  - If the applicant provides information of the data use to the corresponding subjects, they need to define "how" they provided this information (e.g. via shared information of the data use on a project website), otherwise, they need to define the reason "why not".
- The applicant indicated the size of the required study cohort (exact or estimated) and justified this size.
  - Size of the study cohort: it should describe the number of participants.
  - Why does the applicant need a study cohort of this size for the project: the size of the defined study cohort should be justified.
- The applicant specified the time period for the data needed.
  - For which time period(s) will the data be extracted: start and end dates should be defined.
  - Relevance of the time period for the chosen purpose and project's needs are assessed during the assessment phase.
- The applicant defined the required extraction method (random sample, all qualifying individuals, other).
  - If 'random sample' or 'other sample' is defined,
    - The applicant defines the sample size: the number of participants should be described.
  - If 'other sample' is defined,
    - The applicant describes the sample method: the data extraction method should be described.
- The applicant defined how often the data need to be extracted (once or multiple times) and provided information on the study cohort extracting periods/times.
  - If 'multiple times' is selected and the data need to be extracted every 'other' period, the applicant needs to define the other period.
  - More information on the study cohort extracting periods/times: the information should be related to the extracting periods/times.

- *If the applicant is a public sector body or Union institution, body, office or agency:* this question relates to information concerning the period for which the data can be accessed.

- If the applicant's study cohort is based on a previously established cohort (study cohort options (ii) and (iii)),
  - if the cohort was formed based on a previously issued permit, the applicant is expected to provide information about the permit: issuer, date, validity period and permit number
  - If the applicant will use a study cohort based on their own previous survey study and the study cohort was formed based on informed consents of study participants, the applicant is expected to attach the consent and information letter sent to the study subjects. In this case, please see the 'Common plausibility checks' (Table 1; attachment).
    - If the applicant will use a study cohort based on their own previous survey study, but the study cohort was not formed based on informed consents of study participant, the applicant is expected to describe how the cohort was obtained and the reasons for the lack of data permit/consent/legal basis. Check that the applicant provided a description that is not just random text.
  - The applicant defined the contact person who will be responsible for delivering the study cohort information to the relevant HDAB. They need to provide the full name, email and phone number of this person. Please see the 'Common plausibility checks' (Table 1; Natural person name, email, phone).

Subsection 6.2 – Defining the extraction criteria for controls:

If the applicant defined extraction criteria for controls:

- If different data will be extracted for controls, compared to the data extracted for the study cohort, the applicant needs to define/describe similar parameters as for the data extracted for the study cohort (please refer to Section 6.1 instructions).
- The applicant defines the size of the control group: it should describe the number of participants.
- The applicant defines how many controls are extracted per person in the study cohort: it should describe the number of controls.
- The applicant defines the inclusion criteria for extraction of controls.
- If the data for controls will not be extracted simultaneously with the study cohort data, the applicant defines how often the data need to be extracted.
  - If 'multiple times' is selected and the data need to be extracted every 'other' period, the applicant needs to define a valid time period.
  - In case of recurrent extraction, the applicant provides information on each data extraction process separately in the order instructions.
- The applicant provides more information on the extracting periods/times: the additional information should be related to the extracting periods/times.

Subsection 6.3 – Defining the extraction criteria for relatives:

If the applicant defined extraction criteria for relatives,

- If different data will be extracted for relatives, compared to the study cohort, the applicant needs to define/describe similar parameters as for the data extracted for the study cohort (please refer to Section 6.1 instructions):
- The applicant defines the relationship of the relatives to the person belonging to the study cohort (e.g. grandparents, biological parents, mother).
- The applicant defines the size of the group of relatives: it should describe the number of participants.
- If the data for relatives will not be extracted simultaneously with the study cohort data, the applicant defines how often the data need to be extracted.
    - If 'multiple times' is selected and the data need to be extracted every 'other' period, the applicant needs to define a valid time period.
    - In case of recurrent extraction, the applicant provides information on each data extraction process separately in the order instructions.
- The applicant provides more information on the extraction periods/times: the additional information should be related to the extraction periods/times.

Section 7 – Other data to be combined

- If the applicant intends to combine data under the EHDS regulation with other datasets they must demonstrate lawful access to the external data. They need to list the other data and provide information on the data and the planned combination method. Check that the following input fields contain plausible values:
    - Other data to be combined and sources of data: Countries, Data holders, Databases/Registries, Datasets/Registers.
    - Information on data to be combined and the planned method is provided: Dataset, Number of the files, Format of the files, Size of the files and Notes.
        - In this phase, only the existence of these information should be checked, no substantive review.
    - If other data permits were issued for the same project, the applicant is expected to fill in the following information for each permit: the Issuer, Date of issue, Expiry date and Identification information.
- If the dataset records involve permits issued by other parties and permit documents were attached: one should be able to open/view the documents, and they should not be empty.
- If the applicant has a pending permit application related to other data to be combined with the application under review, check that plausible values were given to the following fields:
    - Application submission date.
    - Issuer: should include the name of the issuing authority.

Section 8 – Data processing, data protection and safeguards to prevent unauthorised use of data

Check that the applicant provided the following:

- Technical requirements for the SPEs: it should include information on e.g. computational needs such as RAM, processors, storage, software.
- Data access timelines:
    - If the applicant wishes to access the applied data later and not as soon as possible, they need to define a future date: check the “Later, when?” field.
    - What are the estimated start and end dates of the period during which the electronic health data are needed for processing: it must be a future period, start date must follow the expected decision date.
- Data controller identification: (referring to the data controller of the released data, who determines the purposes and means of processing personal data according to GDPR)
    - A data controller can be a natural person or a legal person. Please see the 'Common plausibility checks' (Table 1; natural person name or legal entity).
- The applicant is expected to list the full names, affiliations and e-mail addresses of all the people who will be processing the data and have access to the SPE. At least one entry should be provided. Plausibility check per field:
    - Full Name: see the ‘Common plausibility checks’ (Table1; natural person name).
    - Affiliation: see the ‘Common plausibility checks’ (Table 1; affiliation).
    - E-mail address: see the ‘Common plausibility checks’ (Table 1; e-mail).

5.4.2 Data request -specific checks

Note to the reader: In addition to the checks of Chapter 5.4, the completeness check of data requests should include the following checks, specific for data requests.

Section 6 – Description of the data needed

The applicant provides a description of the required data for each country/HDAB included in their application. Section 6 input fields are organised into four subsections. Check the following for each country/HDAB involved:

Subsection 6 – Description of the data needed

- The applicant provided an answer (not just random text) to the question about the data linkage plan. The plan should describe how the data from various resources will be linked together, e.g. based on a personal identification code or through subject similarity metrics.

Subsection 6.1 – Defining the extraction criteria

- The applicant provided an indication for the size of the cohort.

- The applicant provided a justification for the size of the cohort requested,
- The applicant provided plausible time periods for the dataset's records extraction.
- The applicant provided plausible input for the required fields of the extraction method defined:
    - Random sample: check the sample size provided.
    - All the people fulfilling the criteria.
    - Other sample: check the sample method and sample size provided.
- The applicant provided plausible input for the inclusion criteria of the cohort extraction.
- The applicant included the tabulation plan(s) as attachment(s). Each plan should include plausible input for the following information:
    - Register to be used
    - Possible study cohort
    - Information on the required variables and tables
    - Formation of variables where they cannot be directly accessed from the database
    - Desired direction of aggregation of percentages
    - Order in which tables are generated when previously generated tables are used to create other tables
    - Any other relevant factor related to generating the required tables
- For the extraction and compilation of statistics, if the requested frequency for the data extraction is 'multiple times',
    - the applicant provided additional information related to the extracting periods/times.
    - if the applicant wants the data to be extracted multiple times over a period of time defined as 'other', the applicant provided plausible input for this other period.

5.5 Results of the completeness check and next actions

If the data access application is incomplete, the HDAB shall notify the applicant through the communication channel in use. If the applicant does not complete the application within the given time frame, a data permit shall not be issued [Article 68(4)]. In this case HDABs can issue a decision stating that the application was rejected due to its incompleteness or the applicant's unresponsiveness. Although a similar time frame is not explicitly foreseen in the EHDS Regulation for data requests (as opposed to data access applications), there is no prohibition either. It is therefore possible to apply a similar four-week window to allow modifications or completion of data requests. This would be beneficial for consistency and user experience and can be adopted operationally.

When the application is deemed complete, the HDAB should check whether it concerns only data from one trusted data holder. If that is the case, the assessment will follow the process described in Article 72 and in Chapter 6.3 of this guideline.

Table 3 shows a summary of the possible completeness check results and next actions.

Table 3. Completeness check results and next actions.

Completeness check result	Additional/ revised information required?	Response received	Response quality	Final status	Next action
Complete	No	N/A	N/A	Complete	Application assessment
Incomplete	Yes	Yes (on time)	Acceptable	Complete	
		Yes (on time)	Poor	Incomplete	Reject application
		No (or late)	N/A	Incomplete	

6 Application assessment process

This chapter describes the assessment phase which begins once the application has been deemed complete. It involves a substantive review of the application's content against the legal and procedural criteria set out in Articles 67–69 of the EHDS regulation. The HDAB evaluates whether a data permit can be granted, or a data request can be approved, and the aspects to be taken into consideration during the assessment process differ for a data access application and a data request.

The assessment marks the start of the processing timeline for issuing or refusing a data permit or assessing a data request, as specified in Article 68(4) and Article 69(4). Please see Chapter 8 for information on time frames.

6.1. How to assess a health data access application

Note to the reader: The content of Chapter 6.1 is applicable also to a health data request, unless otherwise stated. Points specific for health data requests are listed in Chapter 6.2.

The numbering refers to the numbering of the sections in the common application forms (Annex 5 for data access application and Annex 6 for data request, respectively).

It must be checked that the application contains all the points presented [Article 67(2)].

Section 2 – Public information of the project

The application has been published already before the completeness check phase, thus there are no points to be checked at this stage, if the requested description or summary has been provided.

If the description or summary has not been provided:

What to check:

- The applicant has the possibility to state that the nature of their data or project does not allow them to provide a description or summary yet (e.g. due to confidentiality concerns in the early stages of the project). In this case, this field will not be reviewed, but the HDAB should make sure that a reasoning is provided.
    - The HDAB should flag the application, noting that project information for public information purposes has not been submitted yet and can be submitted at later stages – after the permit has been issued or post-permit.

Section 3 – Applicant and contact person information

The health data applicant's identity, either a legal or a natural person and the contact details must be included in the application. If the contact person is not the same person as the applicant, information about their relationship, e.g. based on an employment contract, should be available.

Please note that no application appendices to prove this relationship are required, nor checking personal information online. In addition, the applicant is asked to confirm if they are applying on

behalf of a public sector or EU body and if yes, if they are applying for the data to carry out tasks based on the mandate of that organisation. It should also be clearly specified whether the organisation is conducting the study as part of its own responsibilities or on behalf of a third party.

What to check:

- If the applicant is a public sector or EU body: the applicant is eligible for an accelerated access process - please act accordingly.
- What is the relation between the applicant and contact person if they are not the same person? Is the provided explanation on the relationship plausible?

Section 4 – Payment details

The plausibility of the applicant's invoicing information has been reviewed in the application completeness check phase.

Section 5 – Purpose of data use

The purposes for which access to data are applied for are described in Article 53(1) and one or more can be chosen:

a. public interest in the areas of public or occupational health
b. policy-making and regulatory activities
c. statistics
d. education or teaching activities in health or care sectors
e. scientific research related to health or care sectors that contributes to public health or health technology assessments benefiting end-users incl. development and innovation activities and training of algorithms
f. improvement of the delivery of care, of the optimisation of treatment and of the provision of healthcare

What to check:

- Purposes a-c are reserved only for public sector bodies and EU institutions, bodies, offices and agencies – Is/Are the chosen purpose(s) aligned with the applicant type?
- Are all details of the person responsible for the data use given in the application form?
- *Only applicable to data access applications:* The applicant should also provide an 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 chosen purpose(s).
    - This information should be available either in the application form and/or in the project plan or research protocol.

If the purpose of use is scientific research:

What to check:

- Are all details of the person responsible for the research given in the application form?

To check the purposes, the intended use and the expected benefits (*two latter only applicable to data access applications)*, review the application and appendices in the context of the bigger picture:

- Look at the chosen purpose(s) of use, objectives, project description and potential project plan / research protocol and conclude whether they are plausibly consistent and coherent with each other.
    - What questions does the project seek to answer?
    - Scientific research must relate to the health or care sectors, either directly or indirectly (e.g. through environmental, social or economic factors that affect health outcomes). The link may be broad but must be demonstrable and not purely incidental [Recital 61].
    - Do any doubts about hidden prohibited purposes arise? The prohibited purposes are listed in Article 54.

Further guidance on assessing the chosen purpose(s) of use and any signs of prohibited purpose(s) of use is provided in the TEHDAS2 document “M5.2 Guideline for Health Data Access Bodies on allowed purposes and prohibited secondary use according to EHDS”.

Type of data (only applicable to data access applications)

If pseudonymised, individual-level data are applied for, the applicant must justify why the processing cannot be carried out using anonymised data.

What to check:

- Assess whether the applicant needs individual-level data for their project: Could their needs be satisfied with anonymised, aggregated data?
- If individual-level data are necessary: Does the applicant apply for anonymised or pseudonymised individual-level data?
    - If anonymised: No need for additional checks
    - If pseudonymised: Does the application include plausible justifications for applying for pseudonymised data?

When the purpose(s) of use can be achieved with anonymised data according to information provided by applicant, the default position is that HDAB shall provide electronic health data in an anonymised format [Article 68(3)]. If the outcome of the assessment is that anonymised, aggregated-level statistical data would suffice and the applicant agrees to receiving a response in an anonymised format, HDAB shall proceed with application as a data request instead.

Minimum categories of electronic health data for secondary use are described in Article 51 leaving the possibility to member state for providing in their national legislation that additional categories of electronic health data are to be made available for secondary use.

What to check:

- Are there any additional data categories included that are based on national legislation?
    - If yes, please review the requested data based on the requirements of the national legislation

The health data applicant should be qualified in relation to the intended purposes of data use and have appropriate expertise.

What to check:

- HDABs should assess the applicant's expertise on a case-by-case basis, in proportion to the scope and complexity of the application. A brief description of relevant expertise or role, provided in the application form, will usually suffice.
- For more complex applications (e.g. multiple datasets, multi-country access), the HDAB may request further clarification. There is no general requirement to provide CVs or supporting documents.

Section 6 – Description of the data needed

The applicant must provide a description of the requested electronic health data including their scope, time range, format, sources and, if needed, the geographical coverage where such data are requested from health data holders in several member states or from authorised participants in HealthData@EU.

What to check:

- Review the requested data in the context of the dataset being suitable for the applicant's research objectives. Review the requested data as an entity.
- Do the requested datasets appear coherent and sufficient to support the stated project objectives and declared purpose?
- What questions does the applicant want to answer, and is it possible with the requested data?

What to check:

- Is the suggested extraction clear and comprehensive? Are the questions below answered in the application?
    - From which sources the data will be extracted?
    - For which groups the data will be extracted
        - What is the number of target groups? Will data be collected also for controls and/or relatives?
        - Are the inclusion criteria for the groups clear and valid, considering the project's needs?
        - Is the size of the required target group(s) plausibly justified?
        - Can the chosen sampling method be used to answer the project questions?
    - Are time intervals (for which period the data are extracted) clear and valid?
        - Do the data sources contain data for the proposed time interval?
        - Does the applicant state that something specific related to the extraction has been agreed with the health data holder(s)? The HDAB should receive appropriate information about any special adjustments

Ethical aspects (Section 6)

There is a substantial heterogeneity in the way the ethics practices are provided in member states by processing of health data. Therefore, the processing of data must be clearly described and justified in the project plan or research protocol, containing a statement of the ethical considerations involved. If required by the member state law, the project must be submitted for consideration and approval to an ethics committee before the application assessment. Member states may form the ethics bodies as part of the HDAB, or where an assessment by ethics bodies is required under member state law, those bodies shall make their expertise available to the HDAB [Article 55(2)].

When collaborative research is performed internationally, the research protocol must be approved by research ethics committees in all countries where it is required by member state law. The Article 23 of World Medical Association's Declaration of Helsinki determines the approval of the research protocol by research ethics committees in all countries involved, because only a local committee will have sufficient familiarity with local circumstances and context and ensures representation of the local public taking into consideration the ethical, legal and regulatory norms and standards of the country. The provided ethical approval must be checked to make sure it is coherent and in line with the contents of the application.

Further guidance on ethical consideration is found in the TEHDAS2 document "M5.2 Guideline for Health Data Access Bodies on allowed purposes and prohibited secondary use according to EHDS".

What to check:

- Does the member state's national legislation require an approval by an ethics committee for the type of project the permit is applied for?
    - If yes:
        - Check that the approval has been provided, if required.
        - Check that evaluation is coherent and in line with the contents of the application.
    - If no: Check that the ethical considerations have been included somewhere in the application – this can also be part of the attached project plan or research protocol.

Minimisation principle (Section 6)

It needs to be ensured that the requested data (including their linking, where applicable) are necessary, adequate and proportionate for the purpose(s) of use described in the health data access application, considering data minimisation and purpose limitation requirements provided for in Article 66.

What to check:

- Are all the applied data necessary to perform the planned analyses and to answer the planned questions?
- Has the applicant provided sufficient justifications in terms of data minimisation?
- Is the level of detail of the data necessary and adequate for the needs of the project?
    - On what detail level has the applicant requested the data? E.g. in terms of diagnosis data, does the applicant need information on the subtype of a disease or would information on disease group be sufficient?

Further guidance on taking the data minimisation principle into account is provided in the TEHDAS2 document "M7.2 Guideline for Health Data Access Bodies on data minimisation, pseudonymisation, anonymisation and synthetic data".

Linkage methods (only applicable to data access applications)

The applicant must describe how data from different sources will be linked.

What to check:

- Is the described method feasible, considering the data applied for?
- Does the described method ensure that the potential re-identification risk is minimised as much as possible? Are additional safety measures necessary to further mitigate the risk?

Section 7 – Other data to be combined (only applicable to data access applications)

The applicant must provide a description of datasets already held by them or that are obtained from somewhere else, and that the applicant intends to bring into the SPE.

What to check:

- Check that the suggested combination of other data is feasible.
- Take the other data into account when, for example, formulating the HDAB's cost estimate for processing of the data.
- If linking of other data with data obtained through the EHDS regulation is expected, consider whether the linking affects the assessment of data minimisation (e.g. whether the combined datasets include more variables than necessary for the stated purpose, risks of potential re-identification through cross-referencing data points, whether ethical approvals cover the linkage).

Further guidance on processing and combining the datasets is provided in the TEHDAS2 document "M7.5 Guideline on linkage of health datasets".

Section 8 – Data processing, data protection and safeguards to prevent unauthorised use of data *(only applicable to data access applications)*

The HDAB must check that the safeguards planned to prevent any misuse of the electronic health data are proportionate to the risks and that they adequately protect the rights and interests of the health data holder and of the natural persons concerned, including measures to prevent any re-identification of individuals in the dataset (Article 67(2)).

The applicant is asked to name an SPE if they already know which one they would like to use. They must also provide a description of the tools and computing resources needed in the SPE.

What to check:

- Has the applicant named an SPE in the application?
    - If yes, check that a) HDAB is able to provide access to requested SPE and b) that the SPE is suitable for the data they have requested
        - If the suggested SPE is not a viable option, contact the applicant to discuss potential SPEs that are both suitable for applicant's needs and have appropriate security and safety measures.

Time period for data access (Section 8)

The applicant must provide information and a justification of the period during which the electronic health data are needed for processing in an SPE. In addition, they should specify any needs for the data extraction to be postponed and if any inactive data storage period is needed. Please assess if

the time frame is sufficient for the project in question, especially from the point of view of duration of the application assessment and data extraction processes.

What to check:

- For how long a time does the applicant want to process the data? Is the period in line with the project's needs and it is plausibly justified?
    - The data permit can be granted for a maximum period of 10 years, including the inactive storage period [Article 68(12)]. The applicant has the right to apply for extension of a maximum 10 years at the end of the original 10-year period, by providing an amendment application with justifications for the need for extension.

Transfers outside the EU or the EEA (Section 8)

The applicant must state if there are plans to transfer the applied data outside the EU or the European Economic Area (EEA). According to the GDPR, processing personal data from outside the EU or the EEA constitutes data transfer, even if the data is in an SPE. If such transfer is planned, the applicant must state the country/countries outside the EU/EEA in which the data will be processed and the legal basis for the transfer as per the GDPR's Chapter 5.

What to check:

- If there are plans to transfer the data, check the legal basis for transfer: is it plausible for the country/countries where the data are planned to be processed?

Safeguards (Section 8)

What to check:

- The applicant must have ticked all the boxes in the application to state they confirm the statements related to the safeguards related to protecting the data once released.

Identity of the persons with access to data (Section 8)

What to check:

- The application must list all natural persons who would have access to the electronic health data in the SPE if a data permit were issued, along with information on their affiliations and e-mail addresses.

Lawfulness of processing (Section 8)

The processing of the data must also comply with Articles 6(1) and 9 of GDPR: in these articles the different options for the lawful processing are listed and at least one of them must be applicable. The application form includes these options in a format that the applicant can choose one or multiple

ones. Questions related to the legal basis for processing are also asked separately for the other data to be combined.

What to check:

- Check the option(s) of the applicant for legal processing: Is/Are the option(s) feasible for the project?

Possibility to make an exception to opt-out (Section 8)

As laid down in Article 71, natural persons have a right to opt out from the processing of their personal electronic health data for secondary use. Member states can introduce national rules that override individual opt-outs, allowing all data—regardless of an individual's choice to opt out—to be made available for secondary use under the EHDS regulation. However, such mechanism can only be used under strict conditions, stated in Article 71(4), providing suitable measures for protection of the fundamental rights of natural persons.

Data protection authorities are responsible for overseeing opt-out rights under Article 71 and should coordinate with HDABs within their legal mandate.

What to check:

- Has the applicant requested to make all data available – also those to which the natural person has chosen to opt-out?
  - If yes, are the contents of the application in compliance with the respective member state law?

Guidance on how to implement opt-out is provided in the TEHDAS2 document “M8.1 Guideline for Health Data Access Bodies on how to implement opt-out from secondary use of electronic health data”.

Risks (Section 8)

It must be checked that the risks referred to in Article 68(2), meaning risks for national defence, security, public security and public order and the risk of undermining the confidentiality of data in governmental databases of regulatory authorities are taken into consideration. Please note that these risks might be related e.g. to applicant(s), funder(s) or data applied for.

Applicants are expected to declare whether their intended use may relate to any of these sensitive areas. According to Article 68(2), HDAB must refuse access to data if its use poses significant risks to national defence, public security or public order.

This assessment might be burdensome and time-consuming and will require case-by-case consideration. Questions to consider could, for example, be why military health care data are needed, or if narrow extraction criteria are trying to target central political leaders. While the HDAB is not responsible for conducting a full security or national interest assessment, concerning applications should be flagged and referred to the relevant national authority.

In cases where the requested data may include material subject to intellectual property rights or trade secrets, this must be considered during the assessment process (Article 52). As part of the assessment, HDAB should inform the relevant health data holder(s) when contacting them and request confirmation as to whether the data requested contain any elements protected by intellectual property rights or trade secrets (see details in Chapter 6.4).

If such elements are present, HDAB may make the access conditional on appropriate legal, organisational and technical safeguards - these conditions are part of the data permit template (Annex 9) and data request approval template (Annex 10). These may include contractual arrangements between the health data holder and the health data user, specific access conditions in the permit, or exclusion of certain data elements if needed.

If the risks cannot be mitigated appropriately, the HDAB shall refuse the permit.

Further guidance is provided in the TEHDAS2 document “M5.2 Guideline for Health Data Access Bodies on allowed purposes and prohibited secondary use according to EHDS”.

What to check:

- Does the content of the application pose significant risks to national defence, public security or public order?
    - If the application is concerning, please refer it to the relevant national authority.

6.2 How to assess a health data request

Note to the reader: The content of Chapter 6.2 is specific for data requests. The elements considered in Chapter 6.1 are common for both data access applications and data requests, unless otherwise stated.

The numbering refers to the numbering of the sections in the common application forms.

Section 6 – Description of the data needed

The applicant must provide description of the requested electronic health data including their scope, time range, format, sources and, if needed, the geographical coverage where such data are requested from health data holders in several member states or from authorised participants in HealthData@EU. The other points to be considered have been covered in Chapter 6.1.

What to check:

- Review whether the tabulation plan is sufficiently detailed and technically implementable based on the data sources involved?
- Do the data need to be updated during the permit validity period (=the applicant has stated that the data should be extracted multiple times)?
    - If yes: Has the applicant provided relevant specifying information on this?
    - If yes: Is the planned extraction interval feasible?

6.3 Data from trusted health data holders

Member states may establish a procedure where health data holders can apply to be designated as trusted health data holders [Article 72 (2)]. Where an HDAB receives a health data access application or a health data request that only concerns electronic health data held by a trusted health data holder, a simplified procedure for access may be applied.

Health data access applications and health data requests are submitted to the relevant HDAB who then forwards the application to the relevant trusted health data holder after the completeness check. The trusted health data holder assesses the health data access application or health data request against the same criteria the HDAB would. The trusted health data holder then submits their assessment and proposal for decision to the HDAB, who issues the decision. Please note the HDAB is not bound by the proposal.

After the HDAB has made the decision, the trusted health data holder processes the data and provides access in an SPE as stipulated in Article 57(1), points (a)(i) and (b) (Article 72(6)). Please see time frames in Chapter 8.

Further information on trusted health data holder duties can be found in the TEHDAS2 document “M6.1 Guideline for health data holders on making personal and non-personal electronic health data available for reuse”.

6.4 Contacting health data holders

The HDAB contacts the relevant health data holder(s) during the assessment process to verify the feasibility of the requested data extraction and request a fee estimate. HDABs should choose the communication channel with health data holders in line with national procedures – via the DAAMs or another channel.

Specifically, the HDAB must transmit the extraction criteria and technical specifications provided by the applicant (e.g. target cohort, variables requested, time periods) to the health data holder(s). The health data holder may request further information if needed.

To support the applicant on the selection of data, the HDAB should ensure active communication channels between the HDAB, applicant and health data holders during the assessment. HDABs cannot have expertise in the specifics of all data sets available, or all research subjects. The communication should be active already before submission, e.g. in the form of helpdesk services, when the applicant is preparing the application, to guide the applicant to suitable data. This may save time, reduce errors in the applications, reduce the workload for all parties and help the applicant to obtain the objective of the intended work.

Technical feasibility

The health data holder will confirm whether the extraction is technically feasible. If the health data holder finds the applicant's data description insufficient, the applicant can be requested to provide additional information. These may be requested directly from the health data applicant, but the HDAB must be kept informed of these discussions.

Intellectual property rights and trade secrets

The health data holder will identify any parts of the requested data that may be subject to IPR or trade secrets (TS) protection and inform the HDAB accordingly (Article 52). If such elements are present, the HDAB may make the access conditional on appropriate legal, organisational and technical safeguards - these conditions are part of the data permit template (Annex 9). These may include contractual arrangements between the health data holder and the health data applicant, specific access conditions in the permit, or exclusion of certain data elements if needed. If the risks cannot be mitigated appropriately, the HDAB shall refuse the permit.

The European Commission will develop and recommend non-binding models of contractual terms for these arrangements. Key recommendations for these arrangements are provided in Annex 11.

Further guidance is provided in the TEHDAS2 document “M5.2 Guideline for Health Data Access Bodies on allowed purposes and prohibited secondary use according to EHDS”.

Fee estimate for data extraction

The health data holder will calculate and communicate an expected fee estimate associated with the extraction work. More details about fees are available in the TEHDAS2 document “M4.1.1 Guideline on fees related to the EHDS regulation”.

Further information for health data holders about meeting their obligations under the EHDS regulation can be found in the TEHDAS2 document “M6.1 Guideline for health data holders on making personal and non-personal electronic health data available for reuse”.

6.5 Estimated fees

The estimated fees of the applied data permit or data request shall include health data holders’ fees and the HDAB’s data processing fees. The cost estimate must be sent to the health data applicant for confirmation or rejection, while giving a fixed time frame of when the answer is expected. EHDS regulation does not set a specific time frame for this, but the set time frame should consider the requirement of making a decision within three months of the application being deemed complete.

The estimated fees should include fee breakdowns with specific components explaining cost calculations, if possible, including:

- administrative fees (processing, application management),
- data preparation fees (anonymisation, pseudonymisation etc.)

The examples are not exhaustive.

A breakdown of the data preparation fees for each dataset can be provided, if possible, if the health data applicant wants to review the application scope to reduce estimated costs. The applicant may choose to request only datasets with lower estimated fees. At this stage, the applicant shall be informed and given the possibility not to accept the fee estimation and withdraw the application or request [Article 62 (5)]. Regarding this, the fee estimate must identify costs incurred so far and the applicant shall only be charged these. The applicant may also choose to review the application scope to reduce estimated costs, for example by choosing to request only part of the originally requested datasets.

More details about fees are available in the TEHDAS2 document “M4.1.1 Guideline on fees related to the EHDS regulation”.

Further information about pseudonymisation and data processing can be found in the TEHDAS2 document “M7.2 Guideline on data minimisation, pseudonymisation, anonymisation and synthetic data”.

6.6 Issuing a data permit and approving a data request

If the HDAB requires further information during the application assessment, the HDAB can ask the applicant to provide supplements. The HDAB should use its expertise to consider at which point the HDAB has received enough information and justifications from the data applicant to be able to decide on the application. In this consideration, the HDAB profits from comments from the data holders, acquired during the application assessment. In addition, internal discussion within the HDAB may be beneficial to conclude if all necessary information has been received.

Based on the concluded assessment, the HDAB shall decide to grant or refuse access to data. The permit can be granted fully or partially, or access can be denied. A justification must also be provided in the case of a refusal or a partially granted permit. An official data permit decision or data request approval will be issued to the applicant. A data permit template is included as Annex 9. A data request approval template is included as Annex 10. For data requests, EHDS is not as explicit as for data permits, but e.g. articles 60 and 2(2)(u) imply an expectation for a formal approval also for data requests. Although Article 69 is less explicit than Article 68 on formal approvals, Article 69(4) still requires a decision to be issued within three months, justifying the use of a standardised approval format. Please refer to the Annexes 9 and 10 to find further guidance on what information must be included, as each decision (access granted fully, partially or denied) must enclose specific reference points.

The HDAB shall provide the permit to the applicant via the DAAMs or another channel in line with national procedures. In case the project concerns data from multiple countries, the other HDABs should also be informed of the decision (for more information, please refer to Chapter 6.7).

More information about technical details of issuing a permit are available in the TEHDAS2 document “M6.4 Technical Specifications for Data Access Application Management System (DAAMS) for Health Data Access Bodies (HDABs)”.

6.7 Cross-border and multi-country cases

It is possible for applicants to request access to multiple datasets from different member states or from cross-border registries and databases. When applying for datasets for multiple countries, the applicant must apply via the HealthData@EU Central Platform. Applications will be then distributed to the national contact points for further distribution among the national HDAB(s).

The HDAB overseeing the health data holder with which a cross-border registry or database is registered shall be the one to decide on health data access applications. In cases where these registries or databases have joint controllers, the HDAB responsible for granting access shall be one of the member states where one of the joint controllers is established [Article 76 (1)]. Only one HDAB shall be responsible for granting access to a dataset held jointly, ensuring no duplicate or conflicting decisions.

Where registries or databases from several member states organise themselves into a single network of registries or databases at EU level, they may designate a coordinator. The HDAB

responsible for granting access to these data shall be of the member state in which the coordinator of the network is established [Article 76 (2)].

HDABs and authorised participants in HealthData@EU shall inform each other of their decisions granting access to electronic health data. Additionally, other HDABs may take that information into consideration when deciding on granting or refusing access to electronic health data. A data permit issued by one HDAB may benefit from mutual recognition by the other HDABs, allowing for more informed and consistent evaluations [Article 68 (5)]. Mutual recognition is possible but not automatic.

In multi-country cases, HDABs may decide to provide access to electronic health data in the SPE provided by the European Commission [Article 68 (8), Article 75 (9)].

7 Steps after the decision

7.1 Extraction requests for health data holders

Upon issuing a data permit or approving a data request, the HDAB shall immediately request data extraction from the respective health data holder(s) as per Article 60 and Article 68(7) if not otherwise agreed with the health data user or stipulated in the permit.

The request should include:

- A copy of the approved data permit or the approval of the data request
- A clear specification of the required datasets, including scope, format and intended use
- Deadline for extracting the data in this specific case

Further information about data extraction requests for health data holders can be found in the TEHDAS2 document “M6.1 Guideline for health data holders on making personal and non-personal electronic health data available for reuse”.

7.2 Data preparation, sharing and the SPE

After extraction requests have been sent, the following steps take place:

- Health data holders shall put the requested electronic health data at the disposal of HDAB as per the data permit.
- **Data Extraction**: The HDAB must be check that the datasets received from health data holders are technically intact and in accordance with the description of the requested data, e.g. not include any data beyond what the permit or decision requires.
- **Data Formatting and Processing**: The extracted data are processed and formatted by the HDAB to ensure compliance with technical and ethical standards, including harmonisation where it is required and de-identification procedures such as anonymisation or pseudonymisation in accordance with Article 57(1)(b). Some of these actions might be conducted by the health data holder prior to the data delivery to the HDAB, under HDAB oversight. Further information about how data can be linked and steps preceding it are specified in the document "M7.5 Guideline on linkage of health datasets".
- **Data Encryption and Security Measures**: Before transferring data to the SPE, the HDAB must implement encryption and access control mechanisms to prevent unauthorised access, following Article 57(1)(b). Secure logging of data transmission activities must be maintained for audit purposes. The SPE should ensure compliance with the security measures as specified in Article 73(1) to prevent unauthorised access and mitigate potential security threats.
- **Data Transfer to the SPE** *(only applicable in case of a data permit)*: The HDAB securely transfers the prepared dataset to the designated SPE, ensuring compliance with the EHDS regulation’s security requirements of SPEs as specified in Article 73. Further guidance on making data available in the SPEs by the HDABs can be found in the TEHDAS2 document “M7.4 Technical, functional and security specifications of Secure Processing Environments”.

- **Delivery of the result to the applicant** *(*i.e. anonymised and aggregated outputs; *only applicable in case of a data request):* The delivery does not require the use of an SPE, as the final data are non-personal and not subject to GDPR.
- Deletion of data from the SPE must take place within six months of expiry of the related data permit, following Article 68(12).
- The steps taken to create the dataset may be retained by the HDAB at the request of the health data user.
- The health data user may choose to store the dataset in a storage system with reduced capabilities, for a lower fee compared to the SPE used for active processing.

7.3 Invoicing

HDABs and other bodies (e.g. trusted health data holders) are entitled to invoice according to the EHDS regulation. The TEHDAS2 document "M4.1.1 Guideline on fees related to the EHDS regulation" discusses further the different scenarios and provides recommendations for invoicing.

7.4 Communication with the SPE

Permitted and prepared datasets are securely made available to be accessed by the user within the SPE. This takes place through the HDAB, which will provide the users with credentials to identify them as being authorised to access the data within the SPE referred to in the data permit. All communication must at least be monitored and logged by the HDAB. The process must comply with Article 57(1)(a)(i) and Article 73(1). This is further specified in the TEHDAS2 document "M7.1 Guideline on how to use data in a secure processing environment".

7.5 Monitoring

The HDAB must continuously monitor data usage, security and compliance with the conditions set out in the data permit as required by Article 57(1)(a)(ii). Regular audits and security assessments should be performed to remain in compliance with all the security provisions in Article 73.

Processed datasets must be retained only for the period required to fulfil their intended research purpose. Secure disposal procedures must be implemented in compliance with Article 73 to mitigate risks associated with unauthorised data retention.

Any data breaches or misuse must be reported within the GDPR data breach notification timelines to the relevant authorities and documented in accordance with EHDS guidelines and GDPR requirements.

7.6 Process documentation

The HDAB is required to publish an activity report every two years as per Article 59(1). The EHDS regulation specifies that this report must include categories of information related to data access, requests and security measures:

- The number and type of data access applications and data requests processed
- Compliance measures undertaken
- Security incidents and mitigation strategies

- Improvements and future policy recommendations

To comply with Article 59 and Article 67, the HDAB must maintain accurate records of data access applications and data requests, processing activities and security protocols and interactions with health data holders and users. Collaboration with the trusted health data holders is advisable to gather all relevant information.

7.7 Revocation of permit

HDABs have the power to revoke a data permit in cases of non-compliance by a health data user (Article 63(1)).

HDABs should be aware that non-compliance can be in relation to any requirement placed on health data users by Chapter IV of the EHDS regulation and is not limited to misuse of data. It could, for example, relate to non-payment of permit extension fees.

Where the HDAB decides to revoke a data permit, it shall inform the SPE provider, or otherwise take steps to cease processing. The HDAB may also inform the health data holder. When making these notifications to the SPE provider and the health data holder, the HDAB does not have to divulge the reason for revocation – the HDAB should exercise its own judgement on this point.

Enforcement measures taken by the HDAB, including revocation of a data permit, must be notified to other HDABs through the IT tool referred to in Article 63(7) of the EHDS regulation. Further information on the enforcement measures and processes can be found in the TEHDAS2 document “M4.1.2 Guideline on penalties related to the EHDS regulation”.

7.8 Appeal process

All final decisions taken by the HDAB under the EHDS regulation can be subject to appeal, either by the affected health data applicant, health data user or health data holder. National administrative law of the member state where the HDAB is established applies to the appeal process, including procedural rules and jurisdiction. If the decision to be appealed has been made by the UHDAS, the Court of Justice of the EU has the jurisdiction. It is recommended that HDABs include appeal instructions as an annex to each decision as a good administrative practice.

7.9 Amendments to permit

Health data users can apply for amendments to a permit after it has been issued, provided the original legal basis and purpose of use remain unchanged. Thus, HDABs need to introduce a formal amendment process [Article 68(12)].

The health data user must provide justifications for any amendment to the permit. In general, the responsibility should be on health data users to provide comprehensive information at the time of application, rather than relying on requests for amendments to the permit.

Amendment applications can concern extensions to the permit validity and/or updates to the list of people who have access to data in an SPE. Other types of changes to a permit, e.g. changes in the data or the scope, require assessment by the HDAB and thus a new data permit application.

When an amendment application concerns the duration of the permit validity, the HDAB should consider the following:

- In accordance with Article 68(12), the duration of a permit can be extended once, for a maximum of 10 years.
- A request for an extension, including justifications, must be made by the health data user at least one month before the expiry of the permit.
- The HDAB will decide whether to grant an extension and for how long. The duration of the extension should be in relation to the justifications and the reason for which the health data user needs more time to access the data.

Processing amendment applications is an additional use of HDAB resources and may be subject to an additional processing fee. Additional guidance on fees related to permit amendments can be found in the TEHDAS2 document “M4.1.1 Guideline on fees related to the EHDS regulation”.

Extending the duration of the permit can mean extending the time the data are stored in the SPE. The HDAB may charge additional fees to cover storage of the data and SPE use for the additional period. The additional fee should only relate to the period of the extension of the permit and to the assessment of the extension request.

The HDAB should ensure that all archival and modified versions of the permits are retained. The HDAB shall share the updated permit with the health data holder(s), the SPE provider and the health data user.

7.10 Publication of results and outputs from secondary use

HDABs shall ensure that information on the conditions for making electronic health data available for secondary use is publicly accessible, easily searchable by electronic means and available to natural persons in accordance with Article 58.

Health data users must publicly share the results or outputs of their secondary use of data. Any results or output of secondary use must be published within 18 months after the completion of data processing in the SPE or upon receiving the response to the health data request, as mandated by Article 61(4). This will be further described in the upcoming TEHDAS2 document “M8.4 Guideline for data users on handling research outcomes”.

Users must inform the HDAB from which they obtained the data permit about their results and support the HDAB in making this information publicly available, ensuring transparency and compliance with Article 61(4).

HDABs should establish procedures for engagement with health data users about sharing these results. Related guidance will be available in the upcoming TEHDAS2 document “M8.4 Guideline for data users on handling research outcomes”.

7.11 Publishing information on decisions

The HDAB shall publicly disclose approved data permits and health data request approvals as well as refusal decisions, including the reasons for denial (Article 57[j][iii]). Please see time frames in Chapter 8 and the discussion on publishing applications in Chapter 5.1.

More details about publishing requirements will be available in the upcoming TEHDAS2 document ‘’M8.3 Guideline for Health Data Access Bodies on informing natural persons about the use of health data’’.

8 Time frames

8.1 Time frame for completeness check

The EHDS regulation does not set a time frame for the completeness check. However, it gives time frames on granting a data permit regarding a data access application and on assessing a data request.

The starting point for calculating time frames begins upon receiving a complete data access application. From the HDAB's perspective, this means that prior work is needed in terms of ensuring that the application is complete and ready to be processed. Experience has shown that a completeness check is beneficial for optimising resources for all parties in the process. Although for data requests there is no such provision for completeness in the EHDS regulation, it would be beneficial for consistency to process the data requests in a similar fashion to data access applications.

HDABs may set their own target time (e.g. within 5-10 working days) for the completeness check. While these internal targets are not legally binding, they are useful for internal planning and resource management.

The EHDS regulation gives time frames for the applicant to complete missing or invalid information during the completeness check. The HDAB should provide a clear list of missing or incoherent items to the health data applicant and if possible, list all these items at once. The applicant has up to four weeks to provide the required elements, according to Article 68(4). If the information is not provided on time, the HDAB is not required to proceed with the assessment. The four-week period is a single, continuous window.

8.2 Time frame for application assessment

In principle, a data permit, data request approval or refusal shall be given within three months of receiving a complete application. In case of delay, the applicant shall be informed of the reason for the delay. The HDAB may extend the period for responding to a health data access application by three additional months where necessary, considering the urgency and complexity of the data access application and the volume of submitted applications.

The applicant can be asked to provide missing information also during the assessment process. The HDAB may set a time frame for the applicant to respond (e.g. two weeks), although the EHDS does not give one. This same time frame can be used when the cost estimate is sent to the health data applicant for confirmation.

An accelerated data access application procedure shall be provided 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 reserved for these actors [Article 53(1): a. public interest in the areas of public or occupational health, b. policy-making and regulatory activities, c. statistics]. In such cases, the data permit shall be issued or refused within two months of receiving a complete application. The HDAB may extend the period for responding to a health data access application by one additional month where necessary [Article 68 (4]. Therefore, these applications need to be recognised early in the process to make sure the accelerated timeline can be kept.

Regarding data requests, the HDAB must assess (and approve or refuse) the health data request within three months of receiving it.

When an HDAB has forwarded a health data access application or health data request to a trusted health data holder for assessment (see Chapter 6.3), the trusted health data holder submits their assessment and proposal to the HDAB within two months of receiving the application. The HDAB must issue a decision within two months of receiving the assessment.

In line with Recital 74 of the EHDS regulation, HDABs are not required to follow a strict first-in-first-out approach when processing applications. Prioritisation may be applied based on objective and transparent criteria, such as:

- the urgency of the data use (e.g. related to public health emergencies),
- the public interest value of the request,
- the available capacity of the HDAB and complexity of the application.

It is therefore important to design internal procedures that allow identifying high-priority applications early and allocating resources accordingly, while ensuring overall fairness and transparency.

8.3 Time frame summary

The timelines are summarised below in Figure 1 and Table 4.

Figure 1. Illustration of the various workflows within the HealthData@EU infrastructure, detailing the processes for both national and cross-border data requests. It outlines the expected timeframes and duration for each step in these workflows, providing a clear overview of the procedural stages involved (source: M6.2 Draft guideline for data users on good application and access practice).

Table 4. Summary of time frames for each step of the application processing, according to the EHDS regulation.

STEP	TIME FRAME
Concerning all applications	
Time frame for completeness checks	Not defined in the EHDS regulation
HDAB shall make public any health data access application and health data request	Without undue delay after initial reception (prior to the completeness check)
HDAB publishes all data permits issued or health data requests approved as well as refusal decisions, including their justifications	Within 30 working days of the issuance, approval or refusal
Health data applicant can complete the application during assessment when requested by the HDAB	Not defined in the EHDS regulation
Concerning data access applications	

STEP	TIME FRAME
Health data applicant can complete the application during completeness check when requested by the HDAB	Four weeks
Health data applicant can complete the application during assessment when requested by the HDAB	Not defined in the EHDS regulation
HDAB shall issue or refuse a data permit	Normal process: Within three months of receiving a complete application (+ another three months extension period) Notifying the applicant that the extension period is necessary: as soon as possible Accelerated process: Within two months (+ one additional month extension period)
The trusted health data holder submits their assessment and proposal for decision to the HDAB on an application concerning only data from the trusted health data holder	Within two months of receiving the application from the HDAB
HDAB will issue a decision, taking into account the trusted health data holder's proposal	Within two months of receiving the assessment
The data user can request extension of a data permit	At least one month before the expiry of the permit
Concerning data requests	
HDAB shall assess the health data request	Within three months of receipt of the request
HDAB shall provide the response to the health data request to the health data user	Within a further three months

9 Open questions and unresolved issues

1. Should the full applications, data permits and data request approvals be published in the transparency portal or only certain information from these?

If the full documents should be published, sensitive information related to e.g. the persons entitled to process the data, the detailed description of the granted data sets or other sensitive information might need to be transferred to a non-public annex or similar. The HDAB must justify all omissions.

2. EHDS Article 68(2) states that the HDAB shall take into account (a) risks for national defence, security, public security and public order and (b) the risk of undermining the confidentiality of data in governmental databases of regulatory authorities.

What specific points should be considered when assessing the aforementioned risks? On what level these should be assessed?

3. EHDS states that if a data permit needs to be amended, the health data user shall submit an amendment request. Further, EHDS separately mentions two topics that an amendment can concern: extending the data permit validity period once or modifying the authorised persons with access rights to the electronic health data in a secure processing environment.

Should some other aspects of the data permit be subject to amendment requests?

Potential options could include e.g. transferring the data to another secure processing environment, extracting additional variables from the datasets included in the original permit, and extending the period from which the data are extracted (i.e. extracting more data from the datasets included in the original permit). The original datasets and purpose of use should be maintained.

10 References

This guideline refers to the following TEHDAS2 milestones and deliverables:

- M4.1.1 Guideline on fees related to the EHDS regulation
- M4.1.2 Guideline on penalties related to the EHDS regulation
- M5.2 Guideline for Health Data Access Bodies on allowed purposes and prohibited secondary use according to EHDS
- M6.1 Guideline for health data holders on making personal and non-personal electronic health data available for reuse
- M6.2 Guideline for data users on good application and access practice
- M6.4 Technical Specifications for Data Access Application Management System (DAAMS) for Health Data Access Bodies (HDABs)
- M7.1 Guideline on how to use data in a secure processing environment
- M7.2 Guideline for Health Data Access Bodies on data minimisation, pseudonymisation, anonymisation and synthetic data
- M7.4 Technical, functional and security specifications of Secure Processing Environments
- M7.5 Guideline on linkage of health datasets
- M8.1 Guideline for Health Data Access Bodies on how to implement opt-out from secondary use of electronic health data
- M8.3 Guideline for Health Data Access Bodies on informing natural persons about the use of health data
- M8.4 Guideline for data users on handling research outcomes

This guideline refers to the following legislation:

- Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (Text with EEA relevance)
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)
- Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance)

11 Annexes

Annex number	Annex title
1	Public consultation summary
2	Methodology
3	User journey
4	Glossary
5	Data access application template
6	Data request template
7	Checklist for completeness check: Data access application
8	Checklist for completeness check: Data request
9	Data permit template
10	Data request approval template
11	Key recommendations for electronic contractual arrangements
12	Links to the EHDS regulation articles or recitals

Annex 1 Public consultation summary

This section will be written after the public consultation.

Annex 2 Methodology

This document has been created with a collaborative development process by the TEHDAS2 task 6.3 team. The existing application processing guideline of the Finnish Social and Health Data Permit Authority (Findata) was utilised for context and as a starting point in development of the guideline text. The guideline text was developed with two written commenting rounds with the task team and four section-specific workshops led by the major contributors. The DG Santé representatives have also commented on a working draft of the guideline text to ensure alignment with EHDS requirements and to provide expert feedback.

The data access application and data request forms build on the work done in HealthData@EU Pilot project. In this project, the task 7.2 created common data access applications and data requests, following the EHDS proposal and GDPR framework. These two forms balanced between gathering all necessary information for HDABs to evaluate whether to grant the access and being user-friendly to fill in and process. Information from eight European countries were sought for this development process. Based on solid national level experience on granting health data access, Finland and France were leading experts on this matter (source: HealthData@Pilot Deliverable 7.1).

The common data access application form was introduced in Release 2 of the HealthData@EU central platform. The form has thus far been open for comments in Releases 2, 3 and 4 (status in June 2025) and it has been updated by the task 6.3 lead, Findata, according to the comments. The task 6.3 team has also provided expert comments during these rounds. The annexes 5 and 6 of this document show the current versions of the application forms (as in June 2025) with further suggestions for modifications.

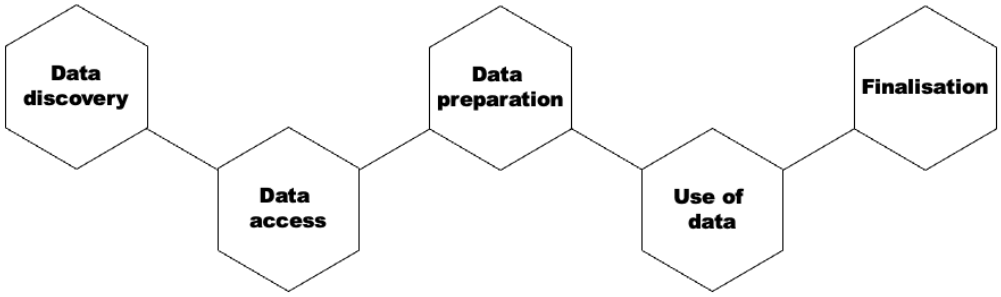
The data permit template was developed with Findata's existing template as a starting point. A commenting round with DG Santé representatives and the task 6.3 team was conducted and the template was further developed by Findata based on the feedback. The data permit template was introduced in Release 4 of the HealthData@EU central platform in May 2025 and has been open for comments there. Annex 9 of this document shows the current version of the data permit template. The data request approval template was developed with Findata's existing template as a starting point in June 2025 after discussion with the DG Santé of the European Commission. The data request approval template is in Annex 10 of this document.

This deliverable will be part of the TEHDAS2 joint action's wave 2 public consultation in September-October 2025.

Annex 3 User journey

When a data user[i] applies for electronic health data for secondary use purposes, such as research and innovation activities, education and policy-making, within the EHDS, the user journey consists of several stages (see Figure 1). Access for certain purposes (public or occupational health, policy-making and regulatory activities and statistics) is reserved for public sector bodies and Union institutions (see Chapter IV, Art. 53(1) and 53(2)).

Figure 1: EHDS user journey consists of five main phases: data discovery, data access, data preparation, use of data and finalisation.



Data discovery

Before being able to use the data, the user needs to investigate whether the data needed is available and whether it is available in the necessary format for the secondary use purpose. This phase is called data discovery. Datasets available in the EU can be found in a metadata catalogue at https://qa.data.health.europa.eu/. Once the data discovery is completed, the user can begin the process of applying for the data.

Data access

In the data access phase, the user fills in and submits a dedicated and standardised data access application form or a data request to a health data access body (HDAB)[ii]. The user must complete the information required in the form, upload necessary documents and provide justifications as needed.

Data access application form is used when the user seeks to use personal level data. **Data request** is for cases when the user wants to apply for anonymised statistical data.

Data preparation

During this phase, the data holder(s)[iii] deliver(s) the necessary data to the HDAB, which starts to prepare the data for secondary use. Techniques for pseudonymisation, anonymisation, generalisation, suppression and randomisation of personal data are

employed. The data minimisation principle (as per the GDPR) must be respected to ensure privacy.

Use of data

In this phase, the user performs analyses based on the received data for the purpose defined in the application phase. Analysing personal level data must be performed in a secure processing environment[iv]. The duration of this phase is specified in the regulation (Art 68(12)).

Finalisation

This last phase of the user journey concerns data user's duties regarding analysis outcomes derived from secondary use of data. Data user must publish the results of secondary use of health data within 18 months of the completion of the data processing in a secure processing environment or of receiving the requested health data. The results should be provided in an anonymous format. The data user must inform the health data access body of the results. In addition, the data user must mention in the output that the results have been obtained by using data in the framework of the EHDS.

Annex 4 Glossary

Project partners have added key terms and their definitions used in the milestones and deliverables to this glossary. The aim is to ensure harmonised terminology in all the TEHDAS2 deliverables.

This is a copy from a living document to be updated throughout the joint action. This version is from 5 September 2025.

Term	Definition
Anonymisation	The process by which personal data is altered in such a way that a data subject can no longer be identified directly or indirectly. (Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, Recital 52; EHDS Regulation, Recital 92)
Anonymous data	Anonymous data is data which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. (Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, Recital 52)
Benefits (of data use)	Refers broadly to positive outcomes of data use. It can encompass social, health and environmental aspects, among others.
Data access	Processing by a data user of data that has been provided by a data holder, in accordance with specific technical, legal, or organisational requirements, without necessarily implying the transmission or downloading of such data. (DGA, Article 2(8),(9) & (13))
Data controller	Data extraction is the process of retrieving data from its source dataset. Structured data extraction involves extracting data from datasets that are already organised in predefined formats. Unstructured data extraction pertains to extracting data from databases handling unstructured formats such as PDFs, images, or free text.

Term	Definition
	There may be one or more different data sources from which data extraction may be required.
Data extraction	Data extraction is the process of retrieving data from its source dataset. Structured data extraction involves extracting data from datasets that are already organised in predefined formats. Unstructured data extraction pertains to extracting data from databases handling unstructured formats such as PDFs, images, or free text. There may be one or more different data sources from which data extraction may be required.
Data linkage	The process of combining datasets ”from several sources on one topic or data subject” (ISO 5127:2017, 3.1.11.12,). This can be done using unique identifiers, probabilistic methods, or a combination of techniques.
Data minimisation	A principle mandating to only collect, store and process personal data in a manner that is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. (GDPR Article 5(1)(c)) Access is only provided to electronic health data that is "adequate, relevant and limited to what is necessary in relation to the purpose of processing indicated in the health data access application by the health data user and in line with the data permit issues pursuant to Article 68.” (EHDS Regulation, Article 66(1)) Data minimisation applies to all stages of the data lifecycle.
Data permit	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 EHDS Regulation. (EHDS Regulation, Article 2(2v))
Data processor	The data processor should handle data exclusively in the manner prescribed by the controller. A data processor acts under the detailed instructions of the data controller only, by processing personal data on their behalf. (GDPR, Article 4(1)(8))

Term	Definition
Data quality	Data quality means the degree to which the elements of electronic health data are suitable for their intended primary use and secondary use; (EHDS Article 2 (2)(z))
Data quality and utility label	Data quality and utility label means a graphic diagram, including a scale, describing the data quality and conditions of use of a dataset. (EHDS Article 2 (2)(aa))
Dataset	A structured collection of electronic health data. (EHDS Article 2(2)(w))
Dataset Catalogue	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. (EHDS Article 2(2)(y))
Dataset subset	Dataset subset contains only selected records from a larger dataset while maintaining its key characteristics and relationships.
Dataset description	Health data access bodies shall, through a publicly available and standardised machine-readable dataset catalogue, provide a description in the form of metadata of the available datasets and their characteristics (EHDS Article (77(1))
Electronic health data	Personal or non-personal electronic health data (EHDS Article 2(2c)).
EU dataset catalogue	A 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. (EHDS Regulation, Article 2 (2y)) The EU dataset catalogue, the national dataset catalogues and the dataset catalogues of authorised participants in HealthData@EU shall be made publicly available. (EHDS Regulation, Article 79 (1–2))
Health data access application	An application seeking to access personal-level electronic health data for secondary use in an anonymised or a pseudonymised format (EHDS Article 67).
Health data access body (HDAB)	Member state-designated authority that facilitates the secondary use of electronic health data. HDABs assess the information provided by the health data applicant and

Term	Definition
	decide on health data requests and access applications, authorise and issue data permits, obtain data from data holders and make data available in Secure Processing Environments. HDABs systematically track the data request and data access applications received and the data permits issued. As per Article 58 of the EHDS, HDABs are required to publicly list information on the data permits issued. (EHDS Article 55 and Recital 52)
Health data applicant	A natural or legal person submitting a health data access application or a data request to a Health Data Access Body for the purposes referred to in Article 53 of EHDS (Article 53).
Health data holder	Any person, organisation or public body involved in healthcare, care services, health-related products, wellness apps or health(care) research, that has the right to process data for health care provision or for public health purposes, reimbursement, research, policy making, official statistics or patient safety. This includes, for example, hospitals, insurers, research institutes and EU institutions. For a more detailed definition: EHDS regulation, Article 2(2)(t)) .
Health data request	A request to access data in an anonymised statistical format for the purposes referred to in EHDS Article 53. (EHDS Article 69)
Health data user	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. (EHDS Article 2(2u))
Intellectual Property (IP)	(a) a trade mark; (b) a design; (c) a copyright or any related right as provided for by national or Union law; (d) a geographical indication; (e) a patent as provided for by national or Union law; (f) a supplementary protection certificate for medicinal products as provided for in Regulation (EC) No 469/2009 of the European Parliament and of the Council of 6 May 2009 concerning the supplementary protection certificate for medicinal products (1); (g) a supplementary protection certificate for plant protection products as provided for in Regulation (EC)

Term	Definition
	No 1610/96 of the European Parliament and of the Council of 23 July 1996 concerning the creation of a supplementary protection certificate for plant protection products (2); (h) a Community plant variety right as provided for in Council Regulation (EC) No 2100/94 of 27 July 1994 on Community plant variety rights (3); (i) a plant variety right as provided for by national law; (j) a topography of semiconductor product as provided for by national or Union law; (k) a utility model in so far as it is protected as an intel lectual property right by national or Union law; (l) a trade name in so far as it is protected as an exclusive intellectual property right by national or Union law;
Interoperability	Ability of organisations, as well as of software applications or devices from the same manufacturer or different manufacturers, to interact through the processes they support, involving the exchange of information and knowledge, without changing the content of the data, between those organisations, software applications or devices. (EHDS Article 2(2f))
Legal basis of data processing	The conditions under which personal data processing is considered lawful (GDPR, Article 6). Purposes for which the electronic health data can be processed for secondary use are laid down in EHDS Article 53.
Metadata	Metadata is a structured and descriptive information about a dataset.
National contact point (NCP)	A National Contact Point for secondary use is the organisational and technical gateway for making electronic health data available for secondary purposes, including research, innovation, policy-making, and public health. It plays a crucial role in connecting national data infrastructures to the HealthData@EU Central Platform, enabling secure and efficient data sharing across borders. (EHDS Regulation Article 75(1))
Non-personal electronic health data	Electronic health data other than personal electronic health data, including both data that have been anonymised so that they no longer relate to an identified or identifiable natural person (the ‘data subject’) and data that have never related to a data subject.

Term	Definition
Personal electronic health data	Data concerning health and genetic data, relating to an identified or identifiable natural person, processed in an electronic form.
Pseudonymisation	T The processing of personal data in such a way that the “data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person. ((Regulation (EU) 2016/679 (GDPR) Article 4(5))
Secondary use	Processing of electronic health data for the purposes set out in Chapter IV of EHDS Regulation, other than the initial purposes for which they were collected or produced. (EHDS Article 2(2e))
Secure Processing Environment (SPE)	An environment in which access to electronic health data can be provided in following a data permit. An SPE is subject to technical and organisational measures and security and interoperability requirements. Specifically allowing access to only those persons listed in the permit, as well as user authentication, authorisation, restricted data handling, logging and the compliance monitoring of respective security measures. (EHDS, Article 73)
Trade secret(s)	Information which meets all of the following requirements: (a) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (b) it has commercial value because it is secret; (c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret;
Transfer of data outside the EU/EEA	General principles, adequacy decisions, appropriate safeguards and specific derogations for transferring personal data to third countries or international organisations (GDPR, Chapter 5, Articles 44–50). The European Data Protection Board (EDPB) identifies three cumulative criteria to identify a transfer outside the EEA: • ”a controller or a processor is subject to the GDPR for the given processing;

Term	Definition
	• this controller or processor discloses by transmission or otherwise makes personal data available to another organisation (controller or processor); • this other organisation is in a country outside EEA or is an international organisation.”
Trusted health data holder	Member State designated health data holder for whom a simplified procedure can be followed for the issuance of data permits. Trusted health data holders leverage their expertise on the data they hold to assist the Health Data Access Body by providing assessments of data requests or access applications. Once data permits are authorised, these trusted data holders provide the data within a Secure Processing Environment that they manage. (EHDS, Article 72 and Recital 76)

Annex 5 Data access application template

This is a test version of a Data Access Application, completed on the HealthData@EU Central Platform (Release 4)

HealthData@EU

The data access application can also be accessed at the HealthData@EU portal: https://acceptance.data.health.europa.eu/. The version available at the portal during the public consultation is Release 5 (published in late September 2025) and it might differ from the Release 4 version shown in this document. This document will be updated with the latest version before final approval.

1. Selecting data sources for the project

About this section

Data users should only apply for data that is adequate, relevant and limited to what is necessary in relation to their purpose of use, following the principle of data minimization of the EU's General Data Protection Regulation 58 (Article 5(1c)). The health data access body evaluates carefully if your requirements are in line with the GDPR data minimization principle.

From which dataset record(s) or register(s) and/or distribution(s) will the data be extracted?

(Filled in automatically based on the data sources selected from the EU Dataset Catalogue)

From which country/countries do you seek data?

(Filled in automatically based on the data sources selected from the EU Dataset Catalogue)

From which data holder(s) will the data be extracted?

(Filled in automatically based on the data sources selected from the EU Dataset Catalogue)

To which health data access body/bodies do you want to submit the application?

(Filled in automatically based on the data sources selected from the EU Dataset Catalogue)

From which database(s) or registry/registries will the data be extracted?

(Filled in automatically based on the data sources selected from the EU Dataset Catalogue)

2. Public information of the project

About this section

The health data access bodies in the European Union are obliged to publish information on the data permits, requests and applications on their website within 30 working days after issuance of the data permit or reply to a data request. In this section, you are asked to provide information on your project that can be shared with the public. Make sure this does not include any confidential information. Provide your answers in layperson's terms. As a data user, you will be obliged to make public the results or output of the project no later than 18 months after the completion of the processing or the receipt of the answer to the data request. In addition, you must inform the health data access body of the number of peer-reviewed research publications, policy documents and/or regulatory procedures conducted using the data accessed via this application.

Project name*

Project leader name (organisation, institution, private sector entity, or a natural person)*

This is the person responsible for data use

Official domicile (country) of the entity responsible for the project*

Purpose for which the data will be used*

Purposes from the EHDS regulation.

Multi-choice radio button (one or more can be chosen):

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 and 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 assessment, or ensures high levels of quality and safety of healthcare, of medicinal products or of medical devices, with the aim of benefitting 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 optimization of treatment and of the provision of healthcare, based on the electronic health data of other natural persons.*

Summary of the project*

☐The nature of your project does not let you provide a summary

(If ticked): **Please explain the reasons why you cannot provide a summary of your project***

This explanation of the reason(s) will not be published.

3. Applicant and contact person information

About this section

A data permit application should state the name and contact details of the applicant, either a legal or a natural person. Information on the contact person responding to any inquiries related to the application, be it the same person as the applicant (in the case of a natural person as the applicant) or another person, should also be included. If the contact person is not the same person as the applicant, their relationship, e.g. based on an employment contract, should be clarified.

Are you applying for data on behalf of a public sector body or a European Union institution, body, office or agency?*

Yes / No

(If yes:) **Are you applying for data for carrying out tasks enshrined in the mandate of your organisation/institution?**

Tasks in your organisation's/institution's mandate mean tasks based on national or European Union law.

Yes / No

Is the applicant a legal or a natural person?

Natural person = a physical person, an individual human being, Legal person = A company, organisation or an association.

Legal person / Natural person *(If you choose this option, you confirm that you apply for data as a private person without any affiliation.)*

Full name

Postal Address

Street name and number

Zip Code

City/Town

Country

Drop-down menu, with distinction into EU/EEA countries and non-EU countries

Contact person information *(title and questions shown only if "legal person" chosen)*

Contact person refers to the person who responds to enquiries concerning the application. The contact person's details can be forwarded to the controller during the processing of an application if additional information is required for defining the data extraction.

Full name

Email (*shown also if "natural person" is chosen)*

Phone (*shown also if "natural person" is chosen)*

Job title

Affiliation

What is the relationship between the contact person and the applicant? (E.g. an employee applying for data on behalf of their organisation.)

Name of the organisation

Business ID of the organisation

4. Payment details

About this section

Payment details of the person to whom the health data access body addresses the bills related to this application and the consequent data permit, if granted.

☐**Same as contact person mentioned in the Section 3?**

Full name

Email

Phone

Name of the organisation *(shown only if "legal person" chosen as applicant in section 3)*

Address

Business ID of the organisation *(shown only if "legal person" chosen as applicant in section 3)*

VAT number *(shown only if "legal person" chosen as applicant in section 3)*

Invoice type

Radio button: Paper or Electronic

Invoice reference number

E-invoice address (EDI or IBAN) *(shown only if "electronic" chosen for invoice type)*

Operator ID *(shown only if "electronic" chosen for invoice type)*

Peppol code (if applicable) *(shown only if "electronic" chosen for invoice type*

Is the project financially covered?

Yes/No

(If yes:) **What is the range of the amount of financing for the project which will use the requested data?**

Drop-down menu: *a. < 10 000 €* *b. 10 000 – 50 000 €* *c. 50 000 – 100 000 €* *d. 100 000 – 500 000 €* *e. 500 000 – 1 000 000 €* f. *> 1 000 000 €*

5. Purpose of data use

About this section

Applicants should indicate the purpose for which data are sought, according to the Article 53(1) of EHDS Regulation corrigendum approved by the European Parliament on 17/12. Applicants need to explain and argue why the requested data are necessary for their indicated purpose of use. Applicants are also asked to provide information on the aim of the project. Then, depending on the use purpose (research or not research), applicants need to provide a summary of the plan for using the data or a summary of the research plan and information on the person responsible for the data use or research.

Purpose of data use. Health data access bodies shall only provide access to electronic health data referred to in Article 51 where the intended purpose of processing pursued by the applicant complies with the following purposes (as per Article 53(1)) listed below).

The chosen purpose(s) of use are copied here from section 2 for reference; the choice cannot be changed here.

Person responsible for the research *(if scientific research chosen as a purpose of use) /* **Person responsible for data use** *(if other purpose(s) is/are chosen)*

☐Same as contact person mentioned in the section 3 (Applicant and contact person information)?

Full name*

Job title*

Affiliation*

Why are the data you are applying for needed for the indicated purpose of use? Explain here why the amount and type of data that you apply for are necessary for your data use purpose*

What is the aim and topic of your project? *

Which is the expected benefit related to the use of the electronic health data and how this benefit contributes to the purposes referred to in 5.1? *

Describe the applicant's qualifications in relation to the intended purpose(s) of data use and appropriate expertise (incl. professional qualifications) *

Provide a summary of your research plan* *(if scientific research chosen as a purpose of use)*

Provide a summary of your plan for using the data* *(if other purpose(s) is/are chosen)*

The summary must be written in one of the official EU languages

Attachment field

Select the language of the summary*

Drop-down menu; official EU languages as options

Select the format of the electronic health data to be made available: *

Anonymised or pseudonymised

If pseudonymised: **I am aware that in order to apply for pseudonymised data, I must:***

Two boxes to be ticked: *a) Explain how I will comply with Article 6(1) of the General Data Protection Regulation (or Article 5(1) of the EU Data Protection Regulation if an EU institution, body, office or agency is applying for data)** *b) Assess ethical aspects of processing the data, where applicable and in line with national law or applicable laws.*

Why do you need pseudonymised data for your project? *

6. Description of the data needed

About this section

In this section, you need to provide a description of the requested dataset, clearly indicating which datasets the application concerns. You should only apply for data that are adequate, relevant and limited to what is necessary in relation to your purpose of use, following the principle of data minimisation of the EU's General Data Protection Regulation (Article 5(1c)). The health data access body evaluates carefully if your requirements are in line with the GDPR data minimisation principle.

Description of the data needed:

To which health data access body do you want to submit the application?

(Filled in automatically based on the data sources selected from the EU Dataset Catalogue)

Respective Dataset Record(s) and Distributions

(Filled in automatically based on the data sources selected from the EU Dataset Catalogue)

If you have been in contact with someone from the health data access body regarding the data you seek, list here the names and the e-mail addresses of this person *

How will the data for one person from different sources be linked? E.g. based on personal identification code. If some kind of other linkage method is used, describe that here *

6.1. Defining the extraction criteria for the cohort: (separate page to be shown for each chosen country)

How is the cohort formed?*

Radio button:

a. *The cohort will be formed based on the criteria given below.*
b. *The cohort has already been formed.*
c. *The cohort will consist of these two: a new cohort formed based on the criteria given below and an already formed cohort.*
d. *The cohort will be the whole population of a country/countries indicated at the beginning of this form.*

Have you provided information of the data use to the corresponding subjects? E.g. shared information of the data use on a project website.*

For further information, see the General Data Protection Regulation articles 13 and 14: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

Yes / No

If yes: **How?***

If no: **Why not?***

<u>If b or c chosen for the question on cohort formation:</u>

If you wish to use a cohort based on your own previous survey study, has the cohort been formed based on informed consents of study participants? E.g. cohort formed based on a survey study or a clinical study, to which register-based data will be linked under the EHDS Regulation.*

Yes / No

If yes: **Does the informed consent cover the requested registry extractions?***

Yes / No

Attach the consent and information letter that you have sent to the study subjects. Do not attach forms that are filled in because they include personal data. *

Only pdf, doc, docx, xls, xlsx, odt files. Maximum size is 5 MB.

Attachment

If "No" to the question on if the cohort is based on a consent:

Has the cohort been based on a data permit granted earlier?*

Yes/No

If yes: **I confirm that the data permit has been granted for this research project***

Yes

If yes: **If the cohort has been formed based on a previously issued permit, list here the following information:**

Issuer of the permit decision

Date

Validity period

From

Date field

To

Date field

Permit number

Attach a permit decision covering the extraction of the cohort data in this section.

Only pdf, doc, docx, xls, xlsx, odt files. Maximum size is 5 MB.

Attachment

If d chosen for the question on cohort formation:

Provide arguments why you need data of a whole population/whole populations? *
Make sure to define the formation of the cohort clearly enough and delimit the cohort size according to the intended use. Pay special attention to which registers the cohort is extracted from and the inclusion and exclusion criteria for the cohort. For example, a geographic definition may mean the place of residence, the place of birth, the place of work, or the place where services are used.

For all options for the question on cohort formation:

Indicate the size of the cohort*

Radio button:* This is an estimation of the size of the cohort.* *or* This is the exact size of the cohort.

Why do you need a cohort of this size for your project?

Ethical review *(questions to be shown based on country choice);*

Only pdf, doc, docx, xls, xlsx, odt files. Maximum size is 5 MB.

Attachment

From which data holder(s) will the data be extracted?

(Filled in automatically based on the data sources selected from the EU Dataset Catalogue)

From which database(s)/registry/registries will the data be extracted?

(Filled in automatically based on the data sources selected from the EU Dataset Catalogue)

From which dataset record(s)/register(s) will the data be extracted?

(Filled in automatically based on the data sources selected from the EU Dataset Catalogue)

If the information is available, attach the list the variables to be used in the data extraction. Use the exact terms provided by the respective data holder(s) in the metadata catalogue.

Only pdf, doc, docx, xls, xlsx, odt files. Maximum size is 5 MB.

Attachment

For which time period(s) will the datasets records be extracted?*

Extraction method*

Radio button:

a. *random sample*
b. *all the people fulfilling the criteria*
c. *other sample*

If a chosen for the question extraction method: **Sample size***

Answers can be for example: 100000 persons or 50% of the people fulfilling the criteria.

<u>If c chosen for the question extraction method:</u>

Describe the sampling method *

Sample size*

Answers can be for example: 100000 persons or 50% of the people fulfilling the criteria.

For all options for the question on extraction method:

Describe the inclusion criteria for cohort extraction

Remember to clarify here any inclusion criteria that may be ambiguous. For example, if you want to include data subjects of certain age, clarify based on which variable the age should be calculated and at which time point.

Describe the potential exclusion criteria for cohort extraction

Data extraction times and order for the cohort

How often does the data need to be extracted?

Radio button: once / multiple times

If multiple times: **The data needs to be extracted every**

If you want the data to be extracted multiple times over a certain period of time, note that the definitions and the data gathering method may change during the review period in some cases. Note that the maximum frequency of data extraction is every quarter

Radio button:

a. *Every year*
b. *Half a year*
c. *Quarter*
d. *Other*

If Other: **Specify Other***

Provide more information on the cohort extracting periods/times*

If it affects the results of the data extraction, in which order will the cohort data be extracted? Provide a numbered list of extraction phases. For example: 1. Data holder A; 2. Data holder B; 3. Data holder C

6.2. Defining the extraction criteria for controls: (separate page to be shown for each chosen country)

Will controls be extracted for the cohort?

Yes / No

If yes: **Has the control group been formed based on a previously issued permit?**

Yes / No

If yes: **If the group of controls has been formed based on a previously issued permit, list here the following information:**

Issuer of the permit decision

Date

Validity period

From

Date field

To

Date field

Permit number

If yes to the first question of this section (Will controls be extracted for the cohort?):

Will same data as for the cohort be extracted for controls?

Yes / No

If no:

From which data holder(s) will the data be extracted?

(Filled in automatically based on the data sources selected from the EU Dataset Catalogue)

From which database(s)/registry/registries will the data be extracted?

(Filled in automatically based on the data sources selected from the EU Dataset Catalogue)

From which dataset record(s)/register(s) will the data be extracted?

(Filled in automatically based on the data sources selected from the EU Dataset Catalogue)

If the information is available, attach the list the variables to be used in the data extraction. Use the exact terms provided by the respective data holder(s) in the metadata catalogue.

Only pdf, doc, docx, xls, xlsx, odt files. Maximum size is 5 MB.

Attachment

For which time period(s) will the datasets records be extracted?*

If yes is answered to the question whether controls are extracted:

Specify the extraction criteria for controls, e.g. matching criteria.

Size of the control group

***Radio button:* This is an estimation of the size of the group of controls* *or* This is the exact size of of the group of controls ***

How many controls are extracted per person belonging to the cohort?

Describe the potential exclusion criteria for controls' extraction

Data extraction times and order for controls

Will the data for controls be extracted at the same time and in the same order as the data for the cohort?

Yes / No

If no, the following questions are shown:

How often does the data need to be extracted?

Radio button: once / multiple times

If multiple times: **The data needs to be extracted every**

If you want the data to be extracted multiple times over a certain period of time, note that the definitions and the data gathering method may change during the review period in some cases. Note that the maximum frequency of data extraction is every quarter

Radio button:

a. *Every year*
b. *Half a year*
c. *Quarter*
d. *Other*

If Other: **Specify Other***

Provide more information on the extracting periods/times*

If it affects the results of the data extraction, in which order will the controls' data be extracted? Provide a numbered list of extraction phases. For example: 1. Data holder A; 2. Data holder B; 3. Data holder C

6.3. **Defining the extraction criteria for relatives**(separate page to be shown for each chosen country)

Will relatives be extracted for the cohort?*

Yes / No

If yes: **Has the group of relatives been formed based on a previously issued permit?***

Yes / No

If yes: **If the group of relatives has been formed based on a previously issued permit, list here the following information*:**

Issuer of the permit decision*

Date*

Validity period

From

Date field

To

Date field

Permit number

If yes to the first question of this section (Will relatives be extracted for the cohort?): **Will same data as for the cohort be extracted for relatives?**

Yes / No

If no:

From which data holder(s) will the data be extracted?

(Filled in automatically based on the data sources selected from the EU Dataset Catalogue)

From which database(s)/registry/registries will the data be extracted?

(Filled in automatically based on the data sources selected from the EU Dataset Catalogue)

From which dataset record(s)/register(s) will the data be extracted?

(Filled in automatically based on the data sources selected from the EU Dataset Catalogue)

If the information is available, attach the list the variables to be used in the data extraction. Use the exact terms provided by the respective data holder(s) in the metadata catalogue.

Only pdf, doc, docx, xls, xlsx, odt files. Maximum size is 5 MB.

Attachment

For which time period(s) will the datasets records be extracted?*

Define the relationship of the relatives to the person belonging to the study cohort (e.g. grandparents, biological parents, mother)

Size of the group of relatives*

Radio button: **This is an estimation of the size of the cohort.*** ***or*** **This is the exact size of the cohort.***

Will the data for relatives be extracted at the same time and in the same order as the data for the cohort?*

Yes / No

If no, the following questions are shown:

How often does the data need to be extracted?*

Radio button: once / multiple times

If multiple times: **The data needs to be extracted every***

If you want the data to be extracted multiple times over a certain period of time, note that the definitions and the data gathering method may change during the review period in some cases. Note that the maximum frequency of data extraction is every quarter

Radio button: *a. Every year* *b. Half a year* *c. Quarter* *d. Other*

If Other: **Specify Other***

Provide more information on the extracting periods/times*

If it affects the results of the data extraction, in which order will the relatives' data be extracted? Provide a numbered list of extraction phases. For example: 1. Data holder A; 2. Data holder B; 3. Data holder C

7. Other data to be combined

About this section

It is possible to combine other personal data, such as data already in your possession or data obtained from elsewhere with another permit, with the data applied for with this application. List the information for all additional data that will be combined with the data authorised by the health data access body. If you later want to combine other personal data with the data authorised by the health data access body, you need to submit an amendment application to the same health data access body. If you have any other cohort that you would like the health data access body to combine with the data you are applying for, you will receive instructions on how to deliver the data securely after the permit has been granted.

Will the data you are applying for be combined with data you have already obtained, or data that will be applied for from other sources?

Yes / No

If yes: **List the other data to be combined and the sources of this data:**

Countries*

Data holders*

Databases/Registries*

Datasets/Registers*

Provide information on data to be combined and the planned combination method*

Provide information on the following, to the extent applicable: dataset, number of the files, format of the files, size of the files, special notes (are there direct/indirect identifiers, data should be pseudonymised, etc.)

List here any other data permits issued for the same project. The permits must be valid at the time data are processed:

Other permits: Issuer of the permit, date of issue, expiry date, permit identification information*

If the dataset records involve permits issued by other parties or they have been collected with consent, attach the permit documents here

Only pdf, doc, docx, xls, xlsx, odt files. Maximum size is 5 MB.

Attachment

Do you have other pending permit applications?

Yes / No

If yes: **List the other data to be combined and the sources of this data:**

Date of submitting the application*

Date field

Issuer*

Permit Identification code

8. Data processing, data protection and safeguards to prevent unauthorized use of data

About this section

According to the EHDS Regulation proposal Article 73(1), the health data access bodies shall provide access to electronic health data only through a secure processing environment.

List here all the technical requirements you have for the secure processing environment.*

If you already know which processing environment you want to use, what is its name and who is it provided by? Provide here the name and the provider of the secure processing environment.*

The health data access body will deliver the data once your application is processed if you are granted a data permit. The health data access body will retain the pseudonymisation key and the extraction terms and documentation used to generate the data. The data permit will be granted only for the duration necessary to fulfil the requested purposes. The permit can be granted for a maximum period of 10 years. This duration may be extended once, at the request of the data user, based on arguments and documents justifying the extension (EHDS Regulation proposal, Article 68(12)). Where needed, the period of use may be extended by applying for an amendment of the data permit.

When do you need the data?*

In general, the health data access body will request the data extraction from the data holders as soon as your application has been processed. If you wish to receive the data later, indicate it here.

Radio button: a. *As soon as possible after this application has been processed* b. *Later, when?*

If later: **Later, when?**

Provide information on the period for which the data can be accessed.*

What is the frequency of that access or the frequency of the data updates?*

If you need to store the data after processing, indicate here the period of inactive data storage

From

Date field

To

Date field

Will the data be transferred outside the EU or the EEA?

The European Data Protection Board (EDPB) has identified three cumulative criteria to qualify a processing operation as a transfer: 1) A controller or a processor ("exporter") is subject to the GDPR for the given processing. 2) The exporter discloses by transmission or otherwise makes personal data, subject to this processing, available to another controller, joint controller or processor ("importer"). 3) The importer is in a third country, irrespective of whether or not this importer is subject to the GDPR for the given processing in accordance with Article 3, or is an international organisation. More information: https://edpb.europa.eu/system/files/2023-02/edpb_guidelines_05-2021_interplay_between_the_applicati on_of_art3-chapter_v_of_the_gdpr_v2_en_0.pdf

Yes/No

In which country/countries outside the EU/EEA will the data be processed?

Multi-choice drop-down menu: all countries outside the EU/EEA

Why will the data be transferred outside the EU or the EEA?

☐Article 47: Transfers on the basis of an adequacy decision

☐Article 48: Transfers subject to appropriate safeguards

☐a. In the absence of a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 or to Article 36(3) of Directive (EU) 2016/680, a controller or processor may transfer personal data to a third country or to an international organisation only if the controller or processor has provided appropriate safeguards and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

☐b. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from the European Data Protection Supervisor, by:

i. A legally binding and enforceable instrument between public authorities or bodies
ii. Standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 96(2)
iii. Standard data protection clauses adopted by the European Data Protection Supervisor and approved by the Commission pursuant to the examination procedure referred to in Article 96(2); L 295/78 EN Official Journal of the European Union 21.11.2018

iv. Where the processor is not a Union institution or body, binding corporate rules, codes of conduct or certification mechanisms pursuant to points (b), (e) and (f) of Article 46(2) of Regulation (EU) 2016/679.

☐c. Subject to the authorisation from the European Data Protection Supervisor, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:

Contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organization.

☐d. Authorisations by the European Data Protection Supervisor on the basis of Article 9(7) of Regulation (EC) No 45/ 2001 shall remain valid until amended, replaced or repealed, if necessary, by the European Data Protection Supervisor.

☐e. The Union institutions and bodies shall inform the European Data Protection Supervisor of the categories of cases in which this Article has been applied.

☐Article 49: Transfers or disclosures not authorised by Union law

What is the legal basis for transferring the data outside the EU or EEA?

More information in the General Data Protection Regulation Chapter 5: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679#d1e4227-1-1

Radio button:

1. *The country/territory/international organisation of transfer ensures an adequate level of protection as per a decision by the European Commission (GDPR Article 35)*
2. *The data controller or processor has provided appropriate safeguards and enforceable data subject rights and effective legal remedies for data subjects are available (GDPR Article 46).*
3. *Other exceptional legal basis (in the absence of appropriate safeguards pursuant to article 46)*

If 2: **These safeguards are provided by***

Multi-choice radio button:

1. *A legally binding and enforceable instrument between public authorities or bodies*

2. *Binding corporate rules in accordance with Article 47*
3. *Standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2)*
4. *Standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2)*
5. *An approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights*
6. *An approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights*

If 3 (to the question What is the legal basis for transferring the data outside the EU or EEA): **Other exceptional legal basis (in the absence of appropriate safeguards pursuant to article 46)**

Multi-choice radio button:

1. *The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguardsBinding corporate rules in accordance with Article 47*
2. *The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request*
3. *The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person*
4. *The transfer is necessary for important reasons of public interes*
5. *The transfer is necessary for the establishment, exercise or defence of legal claims*
6. *The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent*
7. *The transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the*

extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case

Which organisation(s) or individual will be the controller of the data to be formed based on this application?*

A data controller determines the purposes and means of processing personal data. In other words, the data controller decides the how and why of a data processing operation. A data controller can be a legal person, for example a business, an SME, a public authority, an agency or other body. More information: https://edpb.europa.eu/sme-data-protection-guide/data-controller-data-processor_en

How do you comply with the principle of data minimisation (EU Data Protection Regulation) when processing the data?*

EU DPR Article 4(1c) "Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')"

Do you intend to make use of an exception to the right to opt out according to the mechanism provided in the national law of the member state whose data you are applying for?

EHDS article 71(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: (refer to the article for full conditions)"

Yes / No

If yes: **Provide the justification for this exception.**

To proceed with this application, you need to confirm the following statements (data protection and security related statements):*

☐1. I confirm that if the health data access body grants me the data I am applying for, I will use it only for the purpose(s) stated in this application form.*

☐2. I understand that copying the data from the secure processing environment is prohibited.*

☐3. I understand that taking any screenshots or photos of the device screen, once in the secure processing environment, is prohibited.*

☐4. I have sufficient safety measures (such as a firewall) in place to protect the different networks to which the devices used to access the Secure Processing Environment are connected.*

☐5. I understand that re-identification attempts are prohibited and that the health data access body can impose penalties according to Article 43 of the European Health Data Regulation*

Only the people mentioned in the data permit will be granted access to process the data in the secure processing environment.

☐Same as contact person mentioned in the Section 3?

List the full names, affiliations and e-mail addresses of all the people who will be processing the data.*

Lawfulness of processing:

Processing of the personal data that you are applying for with this application form shall be lawful only if and to the extent that at least one of the following applies (in accordance with Article 6(1) of the EU's General Data Protection Regulation, Regulation (EU) 2016/679)*

Multi-choice radio button:

1. *The data subject has given consent to the processing of his or her personal data for one or more specific purposes*
2. *Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract*
3. *Processing is necessary for compliance with a legal obligation to which the controller is subject*
4. *Processing is necessary in order to protect the vital interests of the data subject or of another natural person*
5. *Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*
6. *Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and*

freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Processing of the personal data that you are applying for with this application form shall be lawful only if and to the extent that at least one of the following applies (in accordance with Article 5(1) of the EU's Data Protection Regulation, Regulation (EU) 2018/1725)*

Multi-choice radio button:

1. *Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or bodyProcessing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract*
2. *Processing is necessary for compliance with a legal obligation to which the controller is subject.Processing is necessary in order to protect the vital interests of the data subject or of another natural person*
3. *Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.*
4. *The data subject has given consent to the processing of his or her personal data for one or more specific purposes.*
5. *Processing is necessary in order to protect the vital interests of the data subject or of another natural person.*

What is the legal basis for processing the personal data that you are applying for with this application form?

Multi-choice radio button:

1. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body.
2. Other

If 2: **Other, which?***

What is the legal basis for processing the other data that you will combine with data applied for in this application?

Multi-choice radio button:

1. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body.
2. Other

If 2: **Other, which?***

If purpose of use is scientific research: **If your research requires a research permit from your affiliation organisation, attach the research permit**

Only pdf, doc, docx, xls, xlsx, odt files. Maximum size is 5 MB.

Attachment

9. Additional information

Further information or any additional notes

Here you can provide further information on any of the sections in your application. Indicate the number of section and the question to which your comment refers.

An additional attachment. Do not attach health or personal data to this application.

If you have any other attachment that you deem relevant regarding the processing of your application and necessary for the Health Data Access Body to see, attach it here. Describe its relevance in the text field above.

Only pdf, doc, docx, xls, xlsx, odt files. Maximum size is 5 MB.

Attachment

10. Confirmation of information

About this section

Before this application is processed, you as the applicant must approve processing fees.

To submit your application, you need to confirm the following:

☐I am aware that a processing fee will be charged for processing my application. It will also apply in case of a cancelled request or negative decision.

☐I am aware that data holder(s) may charge a fee.

☐I confirm that the information I have provided is correct.

Annex 6 Data request template

This is a test version of a Data Request Application, completed on the HealthData@EU Central Platform (Release 4)

The data access application can also be accessed at the HealthData@EU portal: https://acceptance.data.health.europa.eu/. The version available at the portal during the public consultation is Release 5 (published in late September 2025) and it might differ from the Release 4 version shown in this document. This document will be updated with the latest version before final approval.

1. Selecting data sources for the project

About this section

Data users should only apply for data that is adequate, relevant and limited to what is necessary in relation to their purpose of use, following the principle of data minimization of the EU's General Data Protection Regulation 58 (Article 5(1c)). The health data access body evaluates carefully if your requirements are in line with the GDPR data minimization principle.

From which dataset record(s) or register(s) and/or distribution(s) will the data be extracted?

(Filled in automatically based on the data sources selected from the EU Dataset Catalogue)

From which country/countries do you seek data?

(Filled in automatically based on the data sources selected from the EU Dataset Catalogue)

From which data holder(s) will the data be extracted?

(Filled in automatically based on the data sources selected from the EU Dataset Catalogue)

To which health data access body/bodies do you want to submit the application?

(Filled in automatically based on the data sources selected from the EU Dataset Catalogue)

From which database(s) or registry/registries will the data be extracted?

(Filled in automatically based on the data sources selected from the EU Dataset Catalogue)

2. Public information of the project

About this section

The health data access bodies in the European Union are obliged to publish information on the data permits, requests and applications on their website within 30 working days after issuance of the data permit or reply to a data request. In this section, you are asked to provide information on your project that can be shared with the public. Make sure this does not include any confidential information. Provide your

answers in layperson's terms. As a data user, you will be obliged to make public the results or output of the project no later than 18 months after the completion of the processing or the receipt of the answer to the data request. In addition, you must inform the health data access body of the number of peer-reviewed research publications, policy documents and/or regulatory procedures conducted using the data accessed via this application.

Project name

Project leader name (organisation, institution, private sector entity, or a natural person)

This is the person responsible for data use

Official domicile (country) of the entity responsible for the project

Purpose for which the data will be used

Purposes from the EHDS regulation.

Multi-choice radio button (one or more can be chosen):

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 and 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 assessment, or ensures high levels of quality and safety of healthcare, of medicinal products or of medical devices, with the aim of benefitting 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 optimization of treatment and of the provision of healthcare, based on the electronic health data of other natural persons.*

Summary of the project

☐The nature of your project does not let you provide a summary

(If ticked): **Please explain the reasons why you cannot provide a summary of your project**

This explanation of the reason(s) will not be published.

3. Applicant and contact person information

About this section

A data request application should state the name and contact details of the applicant, either a legal or a natural person. Information on the contact person responding to any inquiries related to the application, be it the same person as the applicant (in the case of a natural person as the applicant) or another person, should also be included. If the contact person is not the same person as the applicant, their relationship, e.g. based on an employment contract, should be clarified.

Are you applying for data on behalf of a public sector body or a European Union institution, body, office or agency?

Yes / No

(If yes:) **Are you applying for data for carrying out tasks enshrined in the mandate of your organisation/institution?**

Tasks in your organisation's/institution's mandate mean tasks based on national or European Union law.

Yes / No

Is the applicant a legal or a natural person?

Natural person = a physical person, an individual human being, Legal person = A company, organisation or an association.

Legal person / Natural person *(If you choose this option, you confirm that you apply for data as a private person without any affiliation.)*

Full name

Postal Address

Street name and number

Zip Code

City/Town

Country

Drop-down menu, with distinction into EU/EEA countries and non-EU countries

Contact person information *(title and questions shown only if "legal person" chosen)*

Contact person refers to the person who responds to enquiries concerning the application. The contact person's details can be forwarded to the controller during the processing of an application if additional information is required for defining the data extraction.

Full name

Email (*shown also if "natural person" is chosen)*

Phone (*shown also if "natural person" is chosen)*

Job title

Affiliation

What is the relationship between the contact person and the applicant? (E.g. an employee applying for data on behalf of their organisation.)

Name of the organisation

Business ID of the organisation

4. Payment details

About this section

Payment details of the person to whom the health data access body addresses the bills related to this application and the consequent data permit, if granted.

☐Same as contact person mentioned in the Section 3?

Full name

Email

Phone

Name of the organisation *(shown only if "legal person" chosen as applicant in section 3)*

Address

Business ID of the organisation *(shown only if "legal person" chosen as applicant in section 3)*

VAT number *(shown only if "legal person" chosen as applicant in section 3)*

Invoice type

Radio button: Paper or Electronic

Invoice reference number

E-invoice address (EDI or IBAN) *(shown only if "electronic" chosen for invoice type)*

Operator ID *(shown only if "electronic" chosen for invoice type)*

Peppol code (if applicable) *(shown only if "electronic" chosen for invoice type*

Is the project financially covered?

Yes/No

(If yes:) **What is the range of the amount of financing for the project which will use the requested data?**

Drop-down menu:

a. *< 10 000 €*
b. *10 000 – 50 000 €*
c. *50 000 – 100 000 €*
d. *100 000 – 500 000 €*
e. *500 000 – 1 000 000 €*
f. *> 1 000 000 €*

5. Purpose of data use

About this section

Applicants should indicate the purpose for which data are sought, according to the Article 53(1) of EHDS Regulation corrigendum approved by the European Parliament on 17/12. Applicants need to explain and argue why the requested data are necessary for their indicated purpose of use. Applicants are also asked to provide information on the aim of the project. Then, depending on the use purpose (research or not research), applicants need to provide a summary of the plan for using the data or a summary of the research plan and information on the person responsible for the data use or research.

Purpose of data use. Health data access bodies shall only provide access to electronic health data referred to in Article 51 where the intended purpose of processing pursued by the applicant complies with the following purposes (as per Article 53(1)) listed below).

The chosen purpose(s) of use are copied here from section 2 for reference; the choice cannot be changed here.

Person responsible for the research *(if scientific research chosen as a purpose of use) /* **Person responsible for data use** *(if other purpose(s) is/are chosen)*

☐Same as contact person mentioned in the section 3 (Applicant and contact person information)?

Full name*

Job title*

Affiliation*

Why are the data you are applying for needed for the indicated purpose of use? Explain here why the amount and type of data that you apply for are necessary for your data use purpose*

What is the aim and topic of your project? *

Which is the expected benefit related to the use of the electronic health data and how this benefit contributes to the purposes referred to in2? *

Describe the applicant's qualifications in relation to the intended purpose(s) of data use and appropriate expertise (incl. professional qualifications) *

Provide a summary of your research plan* *(if scientific research chosen as a purpose of use*.

Provide a summary of your plan for using the data* *(if other purpose(s) is/are chosen)*

The summary must be written in one of the official EU languages

Attachment field

Select the language of the summary*

Drop-down menu; official EU languages as options

6. Description of the data needed

About this section

In this section, you need to provide a description of the requested dataset, clearly indicating which datasets the application concerns. You should only apply for data that are adequate, relevant and limited to what is necessary in relation to your purpose of use, following the principle of data minimisation of the EU's General Data Protection Regulation (Article 5(1c)). The health data access body evaluates carefully if your requirements are in line with the GDPR data minimisation principle.

Description of the data needed:

To which health data access body do you want to submit the application?

(Filled in automatically based on the data sources selected from the EU Dataset Catalogue)

Respective Dataset Record(s) and Distributions

(Filled in automatically based on the data sources selected from the EU Dataset Catalogue)

If you have been in contact with someone from the health data access body regarding the data you seek, list here the names and the e-mail addresses of this person*

How will the data for one person from different sources be linked? E.g. based on personal identification code. If some kind of other linkage method is used, describe that here'

6.1. **Defining the extraction criteria for the cohort:** (separate page to be shown for each chosen country)

Indicate the size of the cohort*

Radio button:* This is an estimation of the size of the cohort. ***or*** **This is the exact size of the cohort.***

Why do you need a cohort of this size for your project?*

From which data holder(s) will the data be extracted?

(Filled in automatically based on the data sources selected from the EU Dataset Catalogue)

From which database(s)/registry/registries will the data be extracted?

(Filled in automatically based on the data sources selected from the EU Dataset Catalogue).

From which dataset record(s)/register(s) will the data be extracted?

(Filled in automatically based on the data sources selected from the EU Dataset Catalogue)

If the information is available, attach the list the variables to be used in the data extraction. Use the exact terms provided by the respective data holder(s) in the metadata catalogue.

Only pdf, doc, docx, xls, xlsx, odt files. Maximum size is 5 MB.

Attachment

For which time period(s) will the datasets records be extracted?

Extraction method:

Radio button:

a. *random sample*
b. *all the people fulfilling the criteria*
c. *other sample*

If a chosen for the question extraction method: **Sample size***

Answers can be for example: 100000 persons or 50% of the people fulfilling the criteria.

<u>If c chosen for the question extraction method:</u>

Describe the sampling method *

Sample size*

Answers can be for example: 100000 persons or 50% of the people fulfilling the criteria.

For all options for the question on extraction method:

Describe the inclusion criteria for cohort extraction

Remember to clarify here any inclusion criteria that may be ambiguous. For example, if you want to include data subjects of certain age, clarify based on which variable the age should be calculated and at which time point.

Describe the potential exclusion criteria for cohort extraction

Tabulation plan array

In addition, write down the following information for each table: ● register to be used ● possible cohort ● information on the required variables (if available) ● formation of variables where they cannot be directly accessed from the database ● desired direction of aggregation of percentages ● order in which tables are generated when previously generated tables are used to create other tables ● any other relevant factor related to generating the required table(s)

Tabulation plan*

Only pdf, doc, docx, xls, xlsx, odt files. Maximum size is 5 MB.

Attachment

Extraction description and compilation of statistics

A health data access body shall only provide the data you request only in an anonymised statistical format, if your data request is accepted. Due to anonymity, the data user shall have no access to the electronic health data used to provide this answer. All the information you request must be rendered down to a general level in order to avoid small cell counts with high re-identification potential.

How often does the data need to be extracted?

Radio button: once / multiple times

If multiple times: **The data needs to be extracted every**

If you want the data to be extracted multiple times over a certain period of time, note that the definitions and the data gathering method may change during the review period in some cases. Note that the maximum frequency of data extraction is every quarter

Radio button: a. *Every year* b. *Half a year* c. *Quarter* d. *Other*

If Other: **Specify Other***

Provide more information on the cohort extracting periods/times*

Do you intend to make use of an exception to the right to opt out according to the mechanism provided in the national law of the member state whose data you are applying for?

EHDS article 71(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: (refer to the article for full conditions)"

Yes / No

If yes: **Provide the justification for this exception.**

7. Additional information

Further information or any additional notes

Here you can provide further information on any of the sections in your application. Indicate the number of section and the question to which your comment refers.

An additional attachment. Do not attach health or personal data to this application.

If you have any other attachment that you deem relevant regarding the processing of your application and necessary for the Health Data Access Body to see, attach it here. Describe its relevance in the text field above.

Only pdf, doc, docx, xls, xlsx, odt files. Maximum size is 5 MB.

Attachment

8. Confirmation of information

About this section

Before this application is processed, you as the applicant must approve processing fees.

To submit your application, you need to confirm the following:

☐I accept that the health data body will compile the statistics and I will have no access to the data used to form the statistics.

☐I am aware that a processing fee will be charged for processing my application. It will also apply in case of a cancelled request or negative decision.

☐I am aware that data holder(s) may charge a fee.

☐I confirm that the information I have provided is correct.

Annex 7 Checklist for completeness check: Data access application

Completeness checklist (for required fields) DATA ACCESS APPLICATION

Section	Required Field / Group of Fields	Plausibility check	Pass/ Fail
2 – Public information of the project	Project name.	General	
	Project leader name.	Natural person name	
	The reason why applicant cannot provide a description of the data (*if applicable*).	General	
	Summary of the project.	General	
	The reasons why applicant cannot provide a summary of the project (*if applicable*).	General	
3 – Applicant and contact person information	<u>The applicant is a Natural Person:</u>		
	• Applicant name	Natural person name	
	• Postal address	Address	
	• Email	Email	
	• Phone	Phone	
	• Job title	Job title	
	• Affiliation	Affiliation	
	<u>The applicant is a Legal Person:</u>		
	• Applicant name	Legal entity name	
	• Postal address	Address	
	Contact person information:		
	• Full name	Natural person name	

Section	Required Field / Group of Fields	Plausibility check	Pass/ Fail
	• Email	Email	
	• Phone	Phone	
	• Job title	Job title	
	• Affiliation	Affiliation	
	• Relationship between the contact person and the applicant	General	
	• Organization name & Business ID	General	
	• Operator ID	General	
4 – Payment details	Full name	Natural person name	
	Email	Email	
	Phone	Phone	
	Address	Address	
	Invoice reference number	General	
	e-invoice address (EDI or IBAN) (if invoice type is Electronic)	General	
5 – Purpose of data use	Person responsible for data use:		
	• Full name	Natural person name	
	• Job title	Job title	
	• Affiliation	Affiliation	
	Justification of the amount and type of data requested for the data use purpose	General	
	Aim and topic of the project	General	

Section	Required Field / Group of Fields	Plausibility check	Pass/ Fail
	Expected benefit	General	
	Link to the supporting documentation	General	
	Project plan summary attached	Attachment	
	Research plan summary attached	Attachment	
6 – Description of the data needed	Data linkage plan provided	General	
6.1 – Defining the extraction criteria for the study cohort	If the cohort was formed using: (i) criteria from the application form, or, (ii) a previously established cohort, (iii) a combination of options (i) and (ii),		
	If the cohort has been formed based on a previously issued permit, the applicant provides the following information: • Issuer (text) • Date • Validity period (from - to) • Permit number	General	
	Contact person details of the person to deliver the information to the HDAB: • Full name • Email • Phone number	Natural person name Email Phone	
	If the cohort was formed using (ii) a previously established cohort:		

Section	Required Field / Group of Fields	Plausibility check	Pass/ Fail
	If the previous survey study was based on informed consents: • Attach the consent and information letter sent to the study subjects • Attach a permit decision covering the extraction of the cohort data	Attachment Attachment	
	If the previous survey study was NOT based on informed consents: • Describe how the cohort was obtained and the reasons of the lack of data permit/ consent.	General	
	If the cohort was formed using (iv) the whole population of a country/ countries:		
	Arguments were provided to justify the need for the whole populations.	General	
	Size of the cohort	Number	
	Justification for the request cohort size	General	
	The applicant explained how the information of the data use was provided to the corresponding subjects and if not, they provided the reason 'why not'.	General	
	The time period for the data needed was specified.	General	
	The required extraction method and relevant information were specified: • For 'random sample' or 'other sample' the sample size is required.	Number	

Section	Required Field / Group of Fields	Plausibility check	Pass/ Fail
	• For 'other sample' a description of the method is required.	General	
	If the applicant defined 'multiple times' for the frequency of data extraction, over 'Other' period of time, the 'Other' is defined.	General	
	Information on the cohort extracting period/times.	General	
6.2 – Defining the extraction criteria for controls	If the applicant defined extraction criteria for controls:		
	• If different data will be extracted for controls, compared to the data extracted for the study cohort, the applicant defines the same parameters as for the data extracted for the study cohort. You can follow the checklist in 6.1 above.	Checklist point 6.1	
	• Size of the cohort	Number	
	• Number of controls to be extracted per person	Number	
	• Inclusion criteria for control's extraction	General	
	• If the data for the controls will not be extracted simultaneously with the study cohort data, the applicant defines how often the data needs to be extracted:	General	

Section	Required Field / Group of Fields	Plausibility check	Pass/ Fail
	○ If the applicant defined 'multiple times' for the frequency of data extraction, over 'Other' period of time, the 'Other' is defined.		
	• Information on the cohort extracting period/times.	General	
6.3 – Defining the extraction criteria for relatives	If the applicant defined extraction criteria for relatives:		
	• If different data will be extracted for relatives, compared to the study cohort, the applicant defines the same parameters as for the data extracted for the study cohort. You can follow the checklist in 6.1 above.	Checklist point 6.1	
	• The relationship of the relatives to the person belonging to the study cohort.	General	
	• Size of the cohort.	Size	
	• If the data for the relatives will not be extracted simultaneously with the study cohort data, the applicant defines how often the data needs to be extracted: • If the applicant defined 'multiple times' for the frequency of data extraction, over 'Other' period of time, the 'Other' is defined.	General	
Section 7 – Other data to be combined	If the applicant intends to combine EHDS data with other datasets:		
	• Other data to be combined: Countries, Data holders, databases/registries, Datasets/registries.	General	

Section	Required Field / Group of Fields	Plausibility check	Pass/ Fail
	• Information on data to be combined: dataset, number of the files, format of the files, size of the files, notes.	General	
	• If other data permits were issued for the same project the applicant defines the Issuer, Data of issue, Expiry date, identification information.	General	
	• If the dataset records involve permits issued by other parties and permit documents were attached.	Attachment	
	• If the applicant has a pending permit application, • Date of submitting the application • Issuer: the name of the HDAB	General	
Section 8 – Data processing, data protection and safeguards to prevent unauthorized use of data	Technical requirements for the SPE environment	General	
	Data access timelines:		
	• If data access is defined as 'later', the applicant defines 'later, when?'	General	
	• Estimated start and end dates of the period during which the electronic health data is needed for processing	General	
	Data controller identification.	Legal entity	
	People to process the data: • Full name	Natural person name	

Section	Required Field / Group of Fields	Plausibility check	Pass/ Fail
	• Affiliation • E-mail address	Affiliation Email	
	If the applicant's research requires a research permit from their organization they attach the research permit.	Attachment	

Annex 8 Checklist for completeness check: Data request

Completeness checklist (for required fields) DATA REQUEST

Section	Required Field / Group of Fields	Plausibility check	Pass/ Fail
2 – Public information of the project	Project name.	General	
	Project leader name.	Natural person name	
	The reason why applicant cannot provide a description of the data (*if applicable*).	General	
	Summary of the project.	General	
	The reasons why applicant cannot provide a summary of the project (*if applicable*).	General	
3 – Applicant and contact person information	<u>The applicant is a Natural Person:</u>		
	• Applicant name	Natural person name	
	• Postal address	Address	
	• Email	Email	
	• Phone	Phone	
	• Job title	Job title	
	• Affiliation	Affiliation	
	<u>The applicant is a Legal Person:</u>		
	• Applicant name	Legal entity name	
	• Postal address	Address	
	Contact person information:		
	• Full name	Natural person name	

Section	Required Field / Group of Fields	Plausibility check	Pass/ Fail
	• Email	Email	
	• Phone	Phone	
	• Job title	Job title	
	• Affiliation	Affiliation	
	• Relationship between the contact person and the applicant	General	
	• Organization name & Business ID	General	
	• Operator ID	General	
4 – Payment details	Full name	Natural person name	
	Email	Email	
	Phone	Phone	
	Address	Address	
	Invoice reference number	General	
	e-invoice address (EDI or IBAN) (if invoice type is Electronic)	General	
5 – Purpose of data use	Person responsible for data use:		
	Full name	Natural person name	
	Job title	Job title	
	Affiliation	Affiliation	
	Justification of the amount and type of data requested for the data use purpose	General	

Section	Required Field / Group of Fields	Plausibility check	Pass/ Fail
	Aim and topic of the project	General	
	Expected benefit	General	
	Link to the supporting documentation	General	
	Project plan summary attached	Attachment	
	Research plan summary attached	Attachment	
6 – Description of the data needed	Data linkage plan provided	General	
6.1 – Defining the extraction criteria for the study cohort	Size of the cohort.	Number	
	Justification for the size of the cohort request.	General	
	Time periods for the dataset's records extraction.	General	
	If the extraction method defined is 'random sample', the applicant provides the sample size.	Number	
	If the extraction method defined is 'other sample', the applicant provides, • Sample method • Sample size	 General Number	
	Inclusion criteria for the cohort.	General	
	Tabulation plan(s), at least one is provided.	General	
	More information on the extracting periods/times.	General	
	If the data will be extracted multiple times, every 'Other' period of time, the 'Other' is defined.	General	

DECISION
Diary /permit reference number xxxx
Name of the HDAB, country *Date of authorisation*

Annex 9 Data permit template

Your data access application (*application ID/number; date when applied)*

Data permit decision / Decision on data access application, in case of decision refusal

1 ISSUING AUTHORITY

Name of the HDAB

HDAB Contact details; e.g. a general help desk e-mail address

Signature

2 HEALTH DATA USER / HEALTH DATA APPLICANT, in case of decision refusal

Type of user: *Legal person OR natural person*

Name (specify the organisation/consortium name or the natural person's full name)

(if legal person): *Representative's full name and position (and affiliation, if different from the previous line)*

(if scientific research): *Principal investigator; name and affiliation*

The controller of the data to be made available under this data permit is xxx. (In case of joint controllership, please specify all those involved.)

3 REFERENCE

Project title

Permit reference number / diary number
- Only this permit, the potential former permits should be listed in section 5.2
- The HDAB can follow their internal coding system for formulating this number. If such coding system does not exist, it is suggested the reference number should include sequential numbering, the year of submission and the HDAB's country code

Access request / application reference number

4 SUBJECT

The health data user/health data applicant (applicant in case of refusal decision) has applied to the *HDAB name* for a permit to process data in the *project name* pursuant to Article 67 of Regulation (EU) 2025/327 of the European Parliament and of the Council on the European Health Data Space (hereinafter EHDS).

5 DECISION

If permit is granted: Under the EHDS, *HDAB name* grants/partially grants the health data user the permit to process the data referred to in this decision, pursuant to EHDS Article 68 (3). The permit is granted for the project described in the application. HDAB considers the requirements set out in EHDS Article 68(1) to be fulfilled and the risks referred to in Article 68(2) to be sufficiently mitigated. In addition, the requested data are necessary, adequate and proportionate for the purposes described in the health data access application.

If the permit is granted only partially: List further details which aspects are not granted? *Justify reasons for the partial acceptance.*

If permit is refused, option a): Under the EHDS, *HDAB name* refuses the applicant the permit to process the applied data. *Justify reasons for refusal.*

If data permit is refused, option b): response can be given in an anonymised statistical format under Article 69:*HDAB name* grants health data user the permit to process the data referred to in this decision. HDAB considers the requirements set out in EHDS Article 69 to be fulfilled and the risks referred to in Article 68(2) to be sufficiently mitigated.

If permit is granted:

Description of what is decided:

- *the purpose of the study*
- *the method of data collection*
- *the scope of the collected data*
- in case of data matching*: how the data will be matched? Via a identifier available across the datasets or e.g. probabilistic matching?*

- *Mention if this permit is an amendment to an earlier permit.*
- *Access Period: Define the timeframe during which data can be accessed in the SPE.*
- *Retention Period in the SPE: Provide the end date for data retention within the SPE and specify requirements for secure deletion or archiving.*

If trade secrets / IPR right topics need to be considered:

Any trade secrets disclosed as part of the data access process will be handled confidentially and not shared beyond the HDAB name or authorised SPE's name personnel. HDAB name commits to comply with Directive (EU) 2016/943 on the protection of trade secrets.

Data access under this permit does not transfer ownership of any intellectual property.

The data user may develop intellectual property (e.g., algorithms, research findings) based on the data, but must acknowledge the EHDS framework and comply with transparency obligations.

+ add description of specific measures in place for this specific permit

If the mechanism for exception from the right to opt out is used: Pursuant to EHDS Article 71 (4) and the applicable national legislation requirements being met, (specify which) data will be made available to the health data user. Describe here a) the reason for this decision and b) the specific and suitable measures for protecting the fundamental rights and personal data of natural persons as per the applicable national legislation.

If the data are to be combined with those from other country/countries: Description of what data and from which country. If something has been agreed with the other country's/countries' HDAB, elaborate here.

If mutual recognition of another country's HDAB's permit has been done: The data permit *XXX* issued by *name of the other HDAB* has been recognised by *name of the HDAB granting this permit.*

6 JUSTIFICATIONS FOR THE DECISION

6.1 HDAB's (name) competence

Justify why the HDAB is competent to grant the permit: reference(s) to EHDS and/or national legislation

If a trusted data holder has assessed the application and has provided a proposal for the decision*:* trusted data holder name has been designated as a trusted health data holder pursuant to Article 72(2) EHDS by decision reference.

Pursuant to EHDS Article 72(4), HDAB name has forwarded the application to trusted data holder name for assessment on date. The trusted data holder name has provided its assessment and proposal for decision for the HDAB name on date.

6.2 Statements received

List of any relevant other permits, ethical review statements etc.

- *Issuing authority, diary number / permit reference number, issuing date*

Mention, if any of these statements are a prerequisite for the application submission and on the basis of what (e.g. national legislation, or a Member State additional provisions).

If needed, describe the justifications for this decision arising from the other statements.

6.3 Description of the purpose of use

HDAB name grants the health data user a data permit for the following purpose(s), pursuant to EHDS Article 53 (1)) [tick the relevant one(s) below]:

☐ the public interest in the areas of public or occupational health
☐ policy-making and regulatory activities
☐ statistics
☐ education or teaching activities in health or care sectors
☐ scientific research related to health or care sectors
☐ improvement of the delivery of care, of the optimisation of treatment and of the provision of healthcare

Health data user's justifications for the selected purpose(s) of use as provided in the application

Detailed description of the of the purpose for which the data are made available.

The scope and objectives of the project have been verified to be in line with the EHDS

6.4 Data to be disclosed on the basis of the data permit

Data Categories: Clearly define the categories of data to be accessed (e.g., electronic health records, genomic data).

Data Source: Identify the data holder(s) or repository/repositories.

Specify the data to be granted with this permit and how it will be compiled.

The data will be provided in anonymised / pseudonymised format. Justification for providing the data in pseudonymised format.

The detailed description of the data disclosed with this permit is provided in Appendix X.

6.5 Preparing and disclosing of the data

If the HDAB is responsible for pre-processing and disclosing of the data: HDAB name combines, prepares and anonymises/pseudonymises the data.

If a trusted data holder has assessed the application and has provided a proposal for the decision: Pursuant to EHDS Article 72(6), the trusted data holder name is responsible for the preparation and disclosure of the data. The trusted data holder name combines, prepares and anonymises/pseudonymises the data.

6.6 Secure processing environment (section to be included only when individual-level data in anonymized / pseudonymised format will be disclosed)

The data granted with this permit will be released to the *SPE name*.

Description of the responsibilities related to data pre-processing and the chosen SPE

Use of a Secure Processing Environment (SPE): Specify that the data will only be processed in a compliant SPE. Specify which SPE.

Describe the technical characteristics and tools available to the health data user within the chosen secure processing environment and any requirements by the health data user as described in the application.

The health data user is responsible for ensuring compliance with EHDS conditions and applicable laws (e.g., GDPR), prevention of prohibited uses, such as re-identification or unauthorised data transfers. Only anonymous results can be exported from the secure processing environment.

6.7 Producing anonymous results

Further guidance on the anonymous result production

6.8 Persons entitled to process data

The list of persons entitled to process the data granted with this permit is included in the appendix *XX*.

If data are processed from third countries: additional text

7 FEES FOR DATA PERMIT AND DATA PROCESSING SERVICES

Fees for Data Permit and Services

Provide fees in the national currency of the HDAB country.

- *Permit Processing Fee: (e.g., administrative costs for reviewing and issuing the permit).* Note that this may been already paid at the time of submitting the application.

- *Data Preparation Fee: € XX (e.g., anonymization, pseudonymization, data linkage or variable selection).*

- *SPE usage Fee:*
  - *Setup Fee: [€XX] (e.g., initial setup of SPE for project).*
  - *Ongoing Usage Fee: [€XX/day or €XX/hour] (e.g., costs for data storage and computing resources).*
  - *Cold storage*

- *Additional Services (if applicable):*
  - *technical support, additional data modifications, or variable updates.*

- *Fees imposed by the data holders*

***Payment Terms**: indicate payment deadlines, invoicing processes and consequences for late payments.*

***Waivers or Discounts**: Indicate if certain entities (e.g., non-profits, public research bodies) may qualify for reduced or waived fees.*

8 APPLICABLE LEGISLATION

List of applicable legislation, with possibility to add national legislation as well

9 REDRESS MECHANISMS

Further information on claim right

10 APPENDICES

List of appendices; e.g. template for general conditions, with possibility to add national / additional conditions?

DECISION
Diary /permit reference number xxxx
Name of the HDAB, country *Date of authorisation*

Annex 10 Data request approval template

Your data request (*application ID/number; date when applied)*

Decision on generating and disclosing aggregated statistical data

1 ISSUING AUTHORITY

Name of the HDAB

HDAB Contact details; e.g. a general help desk e-mail address

Signature

2 HEALTH DATA USER / HEALTH DATA APPLICANT, in case of decision refusal

Type of user: *Legal person OR natural person*

Name (specify the organisation/consortium name or the natural person's full name)

(if legal person): *Representative's full name and position (and affiliation, if different from the previous line)*

(if scientific research): *Principal investigator; name and affiliation*

3 REFERENCE

Project title

Approval reference number / diary number
- Only this approval
- The HDAB can follow their internal coding system for formulating this number. If such coding system does not exist, it is suggested the reference number should include sequential numbering, the year of submission and the HDAB's country code

Data request reference number

4 SUBJECT

The health data user/health data applicant (applicant in case of refusal decision) has applied to the *HDAB name* for an approval to obtain a response for the *project name* pursuant to Article 69 of Regulation (EU) 2025/327 of the European Parliament and of the Council on the European Health Data Space (hereinafter EHDS).

5 DECISION

DECISION

Diary /permit reference number xxxx

Name of the HDAB, country *Date of authorisation*

If the request is approved: Under the EHDS, *HDAB name* approves/partially approves the health data user's data request to obtain the data referred to in this decision, pursuant to EHDS Article 69. The approval is granted for the project described in the application. The HDAB considers the requirements set out in EHDS Article 69(2) to be fulfilled and the risks referred to in Article 68(2) to be sufficiently mitigated. In addition, the requested data are necessary, adequate and proportionate for the purposes described in the health data request.

If the request is approved only partially: List further details, which aspects are not granted? Justify, why the approval is only partial.

If the request is refused: Under the EHDS, *HDAB name* refuses the applicant the approval to obtain the applied response. *Justify reasons for refusal.*

If the request is approved:

Description of what is decided:

- *the purpose of use of the study*
- *the scope of the collected data*

If trade secrets / IPR right topics need to be considered:

Any trade secrets disclosed as part of the data request process will be handled confidentially and not shared beyond the HDAB name or authorised SPE's name personnel. HDAB name commits to comply with Directive (EU) 2016/943 on the protection of trade secrets.

Obtaining aggregated data under this approval does not transfer ownership of any intellectual property.

The data user may develop intellectual property (e.g., algorithms, research findings) based on the data, but must acknowledge the EHDS framework and comply with transparency obligations.

+ add description of specific measures in place for this specific permit

If the mechanism for exception from the right to opt out is used: Pursuant to EHDS Article 71 (4) and the applicable national legislation requirements being met, (specify which) data will be made available to the health data user. Describe here a) the reason for this decision and b) the specific and suitable measures for protecting the fundamental rights and personal data of natural persons as per the applicable national legislation.

DECISION

Diary /permit reference number xxxx

Name of the HDAB, country *Date of authorisation*

If the data are to be combined with those from other country/countries: Description of what data and from which country. If something has been agreed with the other country's/countries' HDAB, elaborate here.

If mutual recognition of another country's HDAB's approval has been done: The data request approval *XXX* issued by *name of the other HDAB* has been recognised by *name of the HDAB granting this permit.*

6 JUSTIFICATIONS FOR THE DECISION

6.1 HDAB's (name) competence

Justify why the HDAB is competent to grant the approval: reference(s) to EHDS and/or national legislation

If a trusted data holder has assessed the application and has provided a proposal for the decision*:* trusted data holder name has been designated as a trusted health data holder pursuant to Article 72(2) EHDS by decision reference.

Pursuant to EHDS Article 72(4), HDAB name has forwarded the application to trusted data holder name for assessment on date. The trusted data holder name has provided its assessment and proposal for decision for the HDAB name on date.

6.2 Description of the purpose of use

HDAB name grants the health data user the right to obtain statistical aggregated data for the following purpose(s), pursuant to EHDS Article 53 (1) [tick the relevant one(s) below]:

☐ the public interest in the areas of public or occupational health
☐ policy-making and regulatory activities
☐ statistics
☐ education or teaching activities in health or care sectors
☐ scientific research related to health or care sectors
☐ improvement of the delivery of care, of the optimisation of treatment and of the provision of healthcare

Health data user's justifications for the selected purpose(s) of use as provided in the application

Detailed description of the of the purpose for which the data are made available.

The scope and objectives of the project have been verified to be in line with the EHDS Regulation.

6.4 Data to be disclosed on the basis of the data request approval

Data Source: Identify the data holder(s) or repository/repositories.

Specify the data from which the statistical aggregated data will be compiled from.

The data request concerns the data described in more detail in Appendix X and the aggregated statistical data described in Appendix Y.

6.5 Preparing and disclosing of the data

If the HDAB is responsible for pre-processing and producing the anonymous statistical data: HDAB name combines, prepares and produces anonymous aggregated statistical data according to the decision on the tabulation plan.

The aggregated statistical data described in this data request approval will be generated once/quarterly/annually [describe the generation schedule here]. Recurring extractions are carried out on the separate order of the recipient of the decision.

If a trusted data holder has assessed the application and has provided a proposal for the decision*:* Pursuant to EHDS Article 72(6), the trusted data holder name is responsible for the preparation and producing anonymous aggregated statistical data.

7 DECISION FEES AND DATA PROCESSING FEES

Fees:

Provide fees in the national currency of the HDAB country.

- *Decision Fee: (e.g., administrative costs for reviewing and issuing the permit).* Note that this may been already paid at the time of submitting the application.

- *Data Preparation Fee: € XX (e.g., anonymisation, pseudonymisation, data linkage or variable selection).*

- *Additional Services (if applicable):*
  - *technical support, additional data modifications, or variable updates.*

- *Fees imposed by the data holders (e.g. extraction fees)*

***Payment Terms**: indicate payment deadlines, invoicing processes and consequences for late payments.*

***Waivers or Discounts**: Indicate if certain entities (e.g., non-profits, public research bodies) may qualify for reduced or waived fees.*

DECISION

Diary /permit reference number xxxx

Name of the HDAB, country *Date of authorisation*

8 APPLICABLE LEGISLATION

List of applicable legislation, with possibility to add national legislation as well

9 REDRESS MECHANISMS

Further information on claim right

10 APPENDICES

List of appendices; e.g. template for general conditions, with possibility to add national / additional conditions

Annex 11 Key recommendations for electronic contractual arrangements

EHDS Article 52 describes how electronic health data protected by IPR, trade secrets or covered by the regulatory data protection right should be handled and processed in terms of secondary use of data.

Quoting Article 52(4): “When issuing data permits in accordance with Article 68, health data access bodies may make the access to certain electronic health data conditional on legal, organisational and technical measures, which may include contractual arrangements between health data holders and health data users for the sharing of data containing information or content protected by intellectual property rights or trade secrets.”

This annex contains key recommendations for these contractual arrangements. These contractual arrangements are additional to and must not contradict the binding conditions set out in the data permit or the data request approval issued by the HDAB.

When is such contract needed?

Electronic contractual arrangements are required when the requested data

- contain or are derived from trade secrets and/or
- are protected by IPR and/or
- are covered by regulatory data protection right

Who is responsible for creating the contract?

- The European Commission will develop and recommend non-binding models of contractual terms
- The health data holder will create the contract

Who are the parties involved in the contract?

- Data holder whose data are requested
- Data user who is seeking access to these data under the EHDS regulation

What is agreed on?

- Specifications of the data elements being accessed and their protection status (IPR, trade secret, regulatory protection)
- Purpose and scope of data use
    - These must be in line with the permit granted / data request decision made by the HDAB

- Safeguards to prevent disclosure or misuse of confidential information, including technical and legal protection measures
    - General safeguards stipulated in the EHDS regulation are always applicable and those specifically laid down in the data permit / data request decision – this contract should describe any additional safeguards that are necessary considering the specific data elements that fall under intellectual property rights, trade secrets or regulatory data protection
- Any specific access conditions that should be applied beyond those generally applicable under the EHDS framework and the general conditions in the data permit / data request decision
    - These can include but are not limited to access time, technical environment and handling of derived data
- Specific confidentiality and non-disclosure obligations
- Remedies and liability in case of breach or misuse of the protected data
    - Obligation to inform the health data holder of such situations and the actions taken to minimize the consequences as well as to prevent similar events in the future

Who signs the contract?

- The authorised representatives of both the health data holder and the health data user must sign the contract
- Qualified Electronic Signatures (QES) in line with the Regulation (EU) 910/2014 (eIDAS Regulation) to ensure legal recognition across the EU

Additional recommendations:

- Standard template(s) should be used when possible, to ensure consistency and reduce legal inconsistencies
- These contracts should be stored in machine-readable form to support auditability and automation
- The template(s) should be available in all official EU languages

Annex 12 Links to the EHDS regulation articles or recitals

This annex provides information on the legal considerations and the EHDS regulation articles or recitals the guideline refers to.

Referring to Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (Text with EEA relevance), this guideline applies the following articles and recitals:

Recital	Brief description of content
Recital 61	Outlines that “scientific research” within the EHDS regulation includes a wide range of activities with a genuine public benefit.
Recital 70	States that HDABs may charge proportionate, transparent fees to cover operational costs and fees from data holders.
Recital 74	Covers prioritisation rules, extensions of data permits, additional uses, additional fees and harmonisation of data permits.

Chapter I General provisions

Article	**Brief description of content**
Article 2 Definitions	Defines central terms used in the EHDS Regulation.

Chapter IV Secondary use

Section 1: General conditions with regard to secondary use

Article	Brief description of content
Article 51 Minimum categories of electronic health data for secondary use	Describes what categories of electronic health data health data holders shall make available for secondary use.
Article 52 Intellectual property rights and trade secrets	Outlines the tasks of health data holders and HDABs when data subject to intellectual property rights, trade secrets, or regulatory data protection is applied for.
Article 53 Purposes for which electronic health data can be processed for secondary use	Lists lawful purposes of use, for which access to health data can be granted.
Article 54 Prohibited secondary use	Identifies unlawful purposes of use.

Section 2: Governance and mechanisms for secondary use

Article	Brief description of content
Article 55 Health data access bodies	Requires member states to designate independent HDABs responsible for managing tasks related to secondary use of health data.
Article 56 Union health data access service	Establishes a centralized service managed by the European Commission to coordinate access to health data where the health data holders are Union institutions or bodies.
Article 57 Tasks of health data access bodies	Describes the tasks of HDABs related to receiving and deciding on applications.
Article 58 Obligations of health data access bodies towards natural persons	Requires HDABs to respect and protect the rights of natural persons by ensuring transparency, data protection and confidentiality and enabling individuals to exercise their rights.
Article 59 Reporting by health data access bodies	Obliges HDABs to regularly report to their national authorities and the European Commission on the number, type and outcome of secondary-use applications.
Article 60 Duties of health data holders	Requires health data holders to provide timely and accurate electronic health data for secondary use upon request by HDABs.
Article 61 Duties of health data users	Obliges health data users to use secondary-use health data only for the permitted purposes, comply with all conditions set by HDABs and implement appropriate security and confidentiality measures.
Article 62 Fees	Allows HDABs to charge proportionate, transparent fees for processing secondary-use applications, with possible reductions.
Article 63 Enforcement by health data access bodies	Empowers HDABs to monitor and enforce compliance with EHDS rules.

Section 3: Access to electronic health data for secondary use

Article	Brief description of content
Article 66 Data minimisation and purpose limitation	Requires HDABs to ensure that only the minimum necessary and relevant electronic health data are shared for a specific, permitted purpose.

Article 67 Health data access applications	Outlines the requirements for the content of health data access applications, regarding purpose, data needs, safeguards and legal compliance.
Article 68 Data permit	Outlines the conditions under which HDABs assess and issue data permits.
Article 69 Health data request	Allows applicants to request only anonymised statistical responses.
Article 70 Templates to support access to electronic health data for secondary use	Requires the European Commission to adopt standardised templates for health data access applications, data permits and health data requests through implementing acts.
Article 71 Right to opt out from the processing of personal electronic health data for secondary use	Grants individuals the reversible right to opt out of their personal electronic health data being used for secondary purposes.
Article 72 Simplified procedure for access to electronic health data from a trusted health data holder	Allows member states to designate certain health data holders as "trusted," provided they meet strict criteria. Applications or requests for data solely from these trusted holders follow a streamlined process.
Article 73 Secure processing environment	Requires HDABs to provide access to electronic health data exclusively through SPEs that meet strict security standards.

Section 4: Cross-border infrastructure for secondary use

Article	Brief description of content
Article 75 HealthData@EU	Establishes HealthData@EU as a cross-border infrastructure connecting national contact points and participants to facilitate secondary use of electronic health data across the EU.
Article 76 Access to cross-border registries or databases of electronic health data for secondary use	States that the HDAB of the member state where a cross-border registry's health data holder is established shall have the authority to decide on applications concerning that registry.

Section 5: Health data quality and utility for secondary use

Article	Brief description of content
Article 77 Dataset description and dataset catalogue	Requires HDABs to create and publish a standardized catalogue describing available electronic health data sets.
Article 78 Data quality and utility label	Allows health data holders to apply a Union data quality and utility label to datasets.
Article 80 Minimum specifications for datasets of high impact	Empowers the Commission to set minimum specifications for high-impact datasets used for secondary purposes.