M5.2 Draft Guideline for Health Data Access Bodies on minimum categories and limitations on the reuse of health data

Reflections and recommendations for HDABs on allowed purposes and prohibited use according to EHDS

TEHDAS2 – Second Joint Action Towards the European Health Data Space

16 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

Author(s)	Organisation
Nima Andacheh	National Board of Health and Welfare, Sweden
Maria Bergdahl	Swedish eHealth Agency, Sweden
Kristina Bränd Persson	National Board of Health and Welfare, Sweden
Lorenz Dolanski-Aghamanoukjan	Austrian National Public Health Institute (GÖG), Austria
Lisa Ferent	Austrian National Public Health Institute (GÖG), Austria
Ann Gustafsson	Swedish eHealth Agency, Sweden
Gabriella Jansson	Swedish eHealth Agency, Sweden
Christina Jönsson	Swedish eHealth Agency, Sweden
Alexander Leander Knudsen	Danish Health Data Authority, Denmark
Jessica Magnusson	National Board of Health and Welfare, Sweden
Mari Mäkinen	Finnish Institute for Health and Welfare, Finland
Anna Niemeyer	Technology and Methods Platform for Networked Medical Research e.V., Germany
Pieta Näsänen-Gilmore	Finnish Institute for Health and Welfare, Finland
Michael Peolsson	Swedish eHealth Agency, Sweden
Vilma Piironen	Finnish Institute for Health and Welfare, Finland
Marja-Riitta Rautiainen	Finnish Institute for Health and Welfare, Finland
Jenina Soimala	Finnish Institute for Health and Welfare, Finland

0.2 Keywords

Keywords	TEHDAS2, Joint Action, Health Data, European Health Data Space, Purposes and Prohibited secondary use

0.3 Document history

Date	Version	Editor	Change	Status
08/04/2025	0.1	Michael Peolsson	Initial document creation	Draft
07/05/2025	0.2	Ann Gustafsson	Structure Headings	Draft
06/06/2025	0.3	Ann Gustafsson, Gabriella Jansson, Michael Peolsson	Review board	Very first draft
01/07/2025	0.4	Ann Gustafsson, Gabriella Jansson, Michael Peolsson	Final draft	Milestone report
07/09/2025	0.5	Ann Gustafsson	Final draft for approval PSG	Milestone report

Accepted in Project Steering Group on 11092025

Contents

1 Executive summary

This guideline supports the implementation of Articles 53 and 54 of the European Health Data Space regulation (EU) 2025/327 (EHDS regulation), which define the permitted and prohibited purposes for the secondary use of electronic health data. It also addresses Article 52(3), which outlines limitations on the availability of data due to intellectual property rights (IPR) and trade secrets.

The document is intended for Health Data Access Bodies (HDABs), to support consistent, lawful, and efficient assessments of data access applications. It helps HDABs distinguish between the six allowed purposes under Article 53 — including scientific research, public interest, and education — and the prohibited uses listed in Article 54, such as discriminatory practices or the development of harmful products or services.

Articles 53 and 54 should be read together, when HDABs assess an application for access to electronic health data. That is, an HDAB should conclude not only that the purposes described in a health data access application or health data request correspond to one or more of the purposes listed in Article 53 but also that nothing in the applications indicates an infringement with the prohibited secondary uses in Article 54. Hence, it requires careful analysis of the application narrative and any clarifications provided by the applicant.

Although not part of the legal grounds to assess permitted or prohibited purposes under Articles 53 and 54, Article 52(3) is relevant when a lawful purpose cannot be implemented due to unresolved IPR or trade secret concerns. HDABs are responsible for ensuring that all necessary and adequate safeguards are imposed to preserve the confidentiality of IPR. If HDABs conclude that there are insufficient safeguards to protect IPR or trade secrets, it may reject the permit application on these grounds (Article 52(5)).

2 Introduction

2.1 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 data holders, data users and the new health data access bodies in fulfilling their responsibilities and obligations outlined in the European Health Data Space (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 is 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.

2.2 Purpose and context of the guideline

This document provides guidance for HDABs on the the interpretation of allowed purposes and the prohibited secondary use of electronic health data, under Article 53 and 54 in the EHDS regulation. Further, Article 52(3) regarding limitations for making health data available for health data users will also be mentioned. For guidance and recommended procedures for HDABs in processing applications for issuing data permits and making decisions on health data requests, see TEHDAS2 task 6.3

HDABs are responsible for managing data access applications, assessing the lawfulness of intended data uses, and issuing data permits. These responsibilities are critical for ensuring regulatory compliance and protecting individuals' rights.

2.3 Connections with other tasks

This guideline is part of a broader series developed under the TEHDAS2 initiative, which supports the implementation of Chapter IV of the EHDS regulation — governing the secondary use of health data. In Table 1, the connections to other tasks in TEHDAS2 are described.

Table 1. Connections to other tasks in TEHDAS2

Task	Description
T 4.2.1	Guidance for HDAB on penalties for non-compliance related to the EHDS regulation
T 4.2.2	Guidance for member states on stakeholders' engagement to increase knowledge exchange
T 5.1	Guidance for health data holders on their duties to describe data
T 6.2	Guidance for data users on good application and access practice
T 6.3	Guidance for HDAB on processing access applications

2.4 EHDS regulation and secondary use

The secondary use of electronic health data is based on pseudonymised or anonymised data, in order to preclude the identification of the data subjects (Recital 53 in the EHDS regulation).

According to Recital 52, the EHDS regulation provides for a legal basis for the secondary use of personal electronic health data, including the safeguards required under Article 9(2)(g–j) GDPR, to allow the processing of special categories of data.

In addition, the HDAB should assess the information provided by the health data applicant, based on which it should be able to issue a data permit for the processing of personal electronic health data pursuant to the EHDS regulation.

2.5 Target audience

This guideline is written primarily for HDABs that must interpret Articles 53 and 54 of the EHDS regulation when assessing secondary use data applications. Further, it may also assist others, such as health data holders and health data applicants (researchers, public authorities, life-science companies), policymakers and IT implementers.

2.6 Key terminology

The term health data application(s) or data application(s) is used in this document as a general term that includes both health data requests and health data access applications, if not otherwise stated.

For more terms see TEHDAS2_Glossary_for_Milestones_and_Deliverables.docx

See Annex 4 and Table 2 for a summary of concepts that are defined in legal acts of the EU.

3 Scope

This guideline supports the implementation of Articles 53 and 54 of the EHDS regulation. Furthermore, Article 52(3) regarding limitations for making health data available for health data users will be mentioned. It provides practical guidance to HDABs on how to assess applications for secondary use of electronic health data. The focus is on clarifying allowed purposes for secondary use and prohibited secondary use, to assist HDAB´s in taking decisions that are legally grounded and ethically sound.

Parts of this scope is also elaborated on in WP 4 task 4.2.2 engaging stakeholders through different workshops. The Innovative Health Initiative (IHI) project[1] also touches on this subject.

This guideline covers:

- Interpretation and application of Article 53 (allowed purposes for secondary use) and Article 54 (prohibited secondary use).
- Highlighting limitations for making health data available for health data users under Article 52(3) (iIPR and trade secrets).
- Guidance for HDABs on the process of reviewing health data applications regarding the mentioned articles.
- Clarification of conditions under which data may be lawfully accessed and processed, under Articles 53 and 54.
- Alignment of outputs from related TEHDAS2 deliverables.
- Overview of related articles in the context of Articles 53 and 54.

This guideline does not cover:

- Limitations regarding the availability or access to health data (except in relation to IPR and trade secrets, which are included), for example, when someone has exercised their right to opt out under Article 71.
- Broader EHDS infrastructure topics or services beyond “Data access application management” and “Data permit issuing”.

[1] World Health Organisation, ”Occupational health”, https://www.who.int/health-topics/occupational-health.

4 Assessment in the context of application management by HDAB

The HDAB data access application management process is primarily set out in Articles 67–69 of the EHDS regulation, which define the procedural context that any organisational or technical solution for secondary use data applications must align with. Articles 67 and 69 includes the requirements for the common application forms for data access applications and data requests, respectively, to be used by applicants, and which provides the essential information for the processing of applications. Article 68 governs the issuance of data permits and the associated obligations of HDABs, whereas Article 69 provides similar provisions for data requests.

This information together with details of the data requested are core elements that combined will form the basis of the in-depth assessment by the HDAB, in addition to the provisions regarding data minimisation or other measures for data to be given.

Guidance and recommended procedures for HDABs in the full processing of applications for issuing data permits and making decisions on health data requests can be found in TEHDAS2 task 6.3 with operational guidance regarding interpretation of Articles 67-69, 72 and 73.

4.1 Purpose of data use

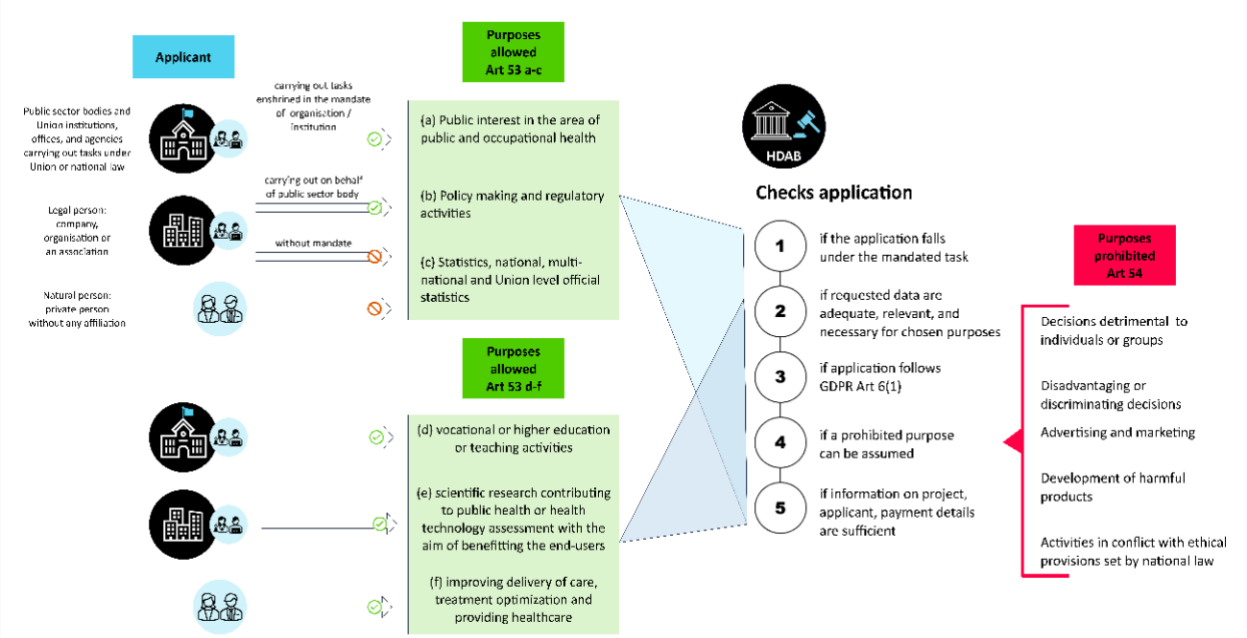
Article 53(1) of the EHDS lays down what to assess: an exhaustive list of six permitted purposes (a–f) for secondary use of electronic health data. Article 53(2) sets the who for part of that list: purposes (a) public/occupational health, (b) policymaking/regulatory tasks, and (c) official statistics are reserved to public-sector bodies and Union institutions (including third parties acting on their behalf), while (d) education, (e) scientific research and innovation (including AI training), and (f) improvement of care are open to all health data users subject to the regulation's general conditions. In applications, the HDAB verifies that the stated purpose is one of the six and clearly specified; if the purpose is (a–c), the HDAB also checks the applicant's legal status/affiliation or mandate authorising that reserved purpose, whereas for (d–f) no special institutional mandate is required and eligibility is assessed on a case-by-case basis (e.g., qualifications and coherence with the stated objectives given the requested access and its complexity). In short: 53(1) defines the purposes; 53(2) limits who may rely on some of them—the distinction is about entitlement, not the legitimacy of the purposes.

According to the procedural context in Article 52(3) we refer to task 6.3.

4.2 Overview of the assessment

Figure 1 (below) shows an overview of the essential information in the application regarding applicants' mandate for the assessment of allowed purposes and prohibited secondary use. It displays who is eligible as an applicant for the different purposes and highlights some of the checks the HDAB needs to do depending on the applicant´s chosen purpose. Further checks that are needed to be done before granting a permit are listed in Article 68, including checking for prohibited purposes (Article 54). (See T6.3 for more details about the full assessment process and checks that HDAB should apply to a data access application or data request, including recommended completeness check procedures.)

Figure 1. Overview of the applicant's mandate and the assessment of allowed purposes a prohibited secondary use of health data. (See Figure 1 enlarged in Annex 5.)



5 General recommendations

This section summarises general recommendations on what HDABs should consider and check for in the assessment process, both with regards to allowed purposes and the prohibited secondary use of electronic health data under Articles 53, 54 and 52(3) in the EHDS regulation. Recommendations specific to certain purposes or prohibited uses will be presented in the below sections (sections 7, 8, and 9).

Articles 53 and 54 should be read together, when HDABs assess an application for access to electronic health data. That is, an HDAB should conclude not only that the purposes described in a health data access application or health data request correspond to one or more of the purposes listed in Article 53(1)(a)–(f) – see Article 68(1)(a) and Article 69(2)(b) – but also that nothing in the applications (or answers to questions following the application) indicates an infringement with the prohibited secondary uses in Article 54. Hence, it requires careful analysis of the application narrative and any clarifications provided by the applicant.

In accordance with the respective roles in the application process, the following general recommendations apply to each role.

5.1 HDABs

- HDABs should make sure that it is understood what an applicant is planning to do with the requested health data (i.e. the aim and intended use), as described in the application, and that at least one of the legal bases under Articles 6 and 9 in the GDPR is at hand.
- It is important that no conclusions based on assumptions should be made. Therefore, depending on the characteristics of the applications, HDABs should take all actions necessary to investigate each application for access to electronic health data, in order to make a thorough assessment, for example:
    - Requesting additional and clarifying information from the data applicant until all questions are answered, and it is possible for the HDAB to take a decision.
    - When necessary, the application can be discussed internally within the HDAB or with other HDABs to identify what information is needed
- HDABs should check if the applicant describes the intended use and expected benefits in the application, in accordance with the chosen purpose(s).
    - The applicant is required to give a detailed explanation of the intended use and expected benefit and how that benefit would contribute to the purpose referred to in Article 53(1), as well as to identify risks and describe proportionate safeguards to prevent misuse (e.g. by serving a prohibited purpose according to Article 54). These requirements are stipulated in Article 67(2)(c) and (g) as well as Article 69(2)(b) and (e) for data access applications and data requests, respectively.
- HDABs should require applicants to clearly and thoroughly specify the intended use of the requested health data, including any potential risks or misuse scenarios, in

accordance with Article 54. The application should include a clear statement of this intended use, accompanied by a binding clause confirming that the data will be used solely for the stated purpose and not for any prohibited secondary uses—such as advertising, marketing, the development of harmful products or services, or other activities restricted under Article 54. These prohibited uses should also be addressed in accompanying guidelines and internal review procedures.

    - For further guidance please see Guideline for HDABs on the procedures and formats for data access (T6.3).

- HDABs should, if not already required under national law, document the assessment, i.e., all documents, communication, investigating steps (for instance contacts with government agencies) and similar in the matter.

    - By doing so, it is possible to monitor compliance with the granted data permit or data request approval, and to get (historical) information on what information the HDAB based its assessment on.

    - It is recommended that the HDABs note (perhaps in a checklist) that Article 54 has been considered in the assessment, before granting a data permit or data request approval.

- Consider setting a common standard for the HDABs´ assessment process regarding for example what basic investigations an HDAB must carry out, for instance regarding the health data user´s company or entity name, what businesses the company or entity, and potential subsidiaries, are running.

5.2 Applicants / health data user

- The applicant should thoroughly specify and clarify in a detailed manner the intended use of the health data that it applied for, and to identify any potential risks or circumstances of misuse in accordance with Article 54.

- A clear explanation of how the declared purpose falls within the applicant's legal remit or delegated mission is required. The burden of proof lies with the applicant. HDABs are not required to investigate or confirm the mandate beyond the information provided.

Thus, it is of utmost importance that member states, in an early stage, ensure that HDABs receive appropriate and coordinated support – ethical, legal, organisational, and technical – to, amongst others, effectively assess electronic health data access applications in line with Articles 53 and 54. Clear procedures for seeking such support should be established. The operationalisation of these support mechanisms remains subject to further development and discussion. For more detail, see section 9.

6 Allowed purposes for secondary use under Article 53

This section provides an analysis of the allowed purposes for secondary use of electronic health data according to Article 53 in the EHDS regulation.

A selection of concepts not previously defined in EU legal acts, based on uncertainties identified during the workshops conducted by task 5.2.1, will also be elaborated.

In some parts, recommendations on what the HDAB should consider and check for in the assessment process with regards to allowed purposes for secondary use of health data will be provided.

6.1 Concepts partially and entirely defined in legal acts of the EU

Several concepts in Article 53 are already defined in legal acts of the EU (see Table 2).

Table 2. Concepts entirely defined in the legal acts of the EU. See Annex 4 for definitions.

Concept	Directive/Regulation
Healthcare	Directive 2011/24/EU, Article 3(a)
Medicinal product	Directive 2011/24/EU referring to Directive 2001/83/EC, Article 1(2)
Medical device	Regulation (EU) 2017/745 and (EU) 2017/746, Article 2(1)
AI systems	AI Act – Regulation (EU) 2024/1689, Article 3(1)
Health technology assessment	Regulation (EU) 2021/2282, Article 2(5)
Areas of Public Health	Regulation (EU) 1338/2008
Areas of Occupational Health	Regulation (EU) 1338/2008, Annex V, (b) and WHO, Article 3(c)2[2]
Serious cross-border threats	Regulation (EU) 2022/2371, Article 2(1)
Public sector body	Regulation (EU) 2022/868, Data Governance Act, Article 2(17)
Statistics	Regulation (EU) 223/2009, Article 3(1)

The concept ‘Development activities’ is not clearly defined in any legal act. However, there is a definition of the notion of research and development in Directive 2009/81/EC, Article 1(27):

[2] World Health Organisation, ”Occupational health”, https://www.who.int/health-topics/occupational-health.

"'Research and development' mean all activities comprising fundamental research, applied research and experimental development, where the latter may include the realisation of technological demonstrators, i.e. devices that demonstrate the performance of a new concept or a new technology in a relevant or representative environment."

6.2 Access to health data reserved for public sector bodies

In Article 53(1) the three purposes listed under (a–c) are restricted to public sector bodies as stipulated in Article 53(2) of the EHDS regulation (see the full text of the article in Annex 3).

The applicable definition of a 'public sector body' is provided in Article 2(1)(c) of the EHDS regulation, which refers to Article 2(17) of the Data Governance Act (Regulation (EU) 2022/868): "'Public sector body' means the state, regional or local authorities, bodies governed by public law, or associations formed by one or several such authorities or one or several such bodies governed by public law."

6.2.1 General reflections

Since a member state may mandate other entities to act on its behalf for a specific purpose in the same way as any other contractor, international organisations are not eligible by default and must act through or under a mandate from a public authority.

Because of this prerequisite of unconditional affiliation with a public sector body authorised for these application purposes it is not sufficient for an applicant to be a public sector body or to act on behalf of one — the mandate or delegation must also cover the specific purpose (a)(b) or (c) listed in Article 53(1). The HDAB should assess not only the status or affiliation, but also whether the delegated task explicitly relates to the stated purpose. This is essential to prevent overly broad interpretations of what constitutes public interest or eligibility for policymaking.

Therefore, affiliation with or contracting by a public authority is not sufficient unless the contract or delegation explicitly covers tasks relating to public health, policymaking or statistics.

In validating this requirement, HDABs must verify both

- the applicant's legal status or mandate, and
- that the scope of that mandate covers the stated purpose under Article 53(a–c).

For example: A national health research institute applies for access to conduct public health surveillance. It must provide the national law or governmental decree that legally establishes its role in public health monitoring. If acting under a ministry's mandate, it must provide proof of that.

6.2.2 Recommendations for assessment of purpose and mandate

In order to actually select and apply for data, prior login or registration on the data portal is required, during which the affiliation could and should be checked. An automated check during the application process to determine whether the applicant belongs to a public sector body could support the HDABs. In this case, only in the case of a mandate, i.e. an application

on behalf of a public sector body, would it be necessary to provide suitable evidence and check this manually.

- HDABs should verify both
  - the applicant's legal status or mandate, and
  - that the scope of that mandate covers the stated purpose under Article 53(a–c).
- HDABs are not required to investigate or confirm the mandate beyond what is submitted.
  - The burden of proof lies with the applicant. Applicants should provide documentation such as proof of legal status as a public sector body (e.g. statute, legal register).
  - In the case of delegated tasks: a formal contract, agreement, or letter of mandate clearly specifying the task and its relevance to the purpose cited. A clear explanation of how the declared purpose falls within the applicant's legal remit or delegated mission.

6.3 Article 53(1)(a) – Public interest

Article 53(1)(a) of the EHDS regulation permits access to electronic health data when the stated purpose relates to

"[…] 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; […]"

The term 'public interest' is of union law character. It is not defined in any legal act, for instance in the GDPR. However, references to recitals in the EHDS regulation and the GDPR may be useful as guidance for interpreting the provisions (see below).

6.3.1 The concept of "public interest"

The term 'public interest' requires a clear and comprehensible definition, as it forms the basis for the other concepts discussed in this section. It is a widely used and at the same time controversial term for which there is no clear and precise definition to date.

The lack of a clear, generally applicable definition is countered in the EHDS regulation, among others, by explicitly naming tasks or aspects that the legislator considers to be in the

public interest. The notion of 'public interest' must not be interpreted as a general justification. HDABs should require clear and well-documented evidence demonstrating how the intended purpose satisfies the criteria set out in Article 53(1)(a), and should verify that the applicant is duly entitled to act on this basis

In the EHDS regulation, public interest is often mentioned, notably in Recitals 19, 20, 52, 54, 95 and 100.

Recital 52 of the EHDS regulation makes reference to the allocations in the GDPR:

"[...] This Regulation also assigns tasks in the public interest within the meaning of Article 6(1)(e), of Regulation (EU) 2016/679 to the health data access bodies and meets the requirements of Article 9(2) (g–j), as applicable, of that Regulation. […]"

Recital 61 of the EHDS regulation describes the objectives to be achieved by enabling secondary use of the data. The overarching objective here is the following:

"[…] In particular, the secondary use of health data for research and development purposes should contribute to benefiting society in the form of new medicines, medical devices, and healthcare products and services at affordable and fair prices for Union citizens, as well as to enhancing access to and the availability of such products and services in all member states. […]"

Tasks and activities that serve these objectives or contribute to their fulfilment can therefore be understood as being in the public interest.

The references cited are almost identical to the cases provided for public interest in Recital 54 and Article 53(1)(c) of the EHDS regulation.

Recital 54 of the EHDS regulation specifies which facts are specifically to be assigned to the public interest:

"[…] strong link to the public interest, such as activities for protection against serious cross-border threats to health or scientific research for important reasons of public interest, […]"

Further, in Recital 54, other aspects are mentioned as being in the public interest:

"[…] Scientific research for important reasons of public interest could for example include research addressing unmet medical needs, including for rare diseases, or emerging health threats. […]"

These categorisations are taken up again in Article 53(1)(a) and explicitly named as permitted purposes.

Furthermore, Recital 54 and Article 71 of the EHDS regulation allows that the member states may decide that they are authorised to access relevant data even if an opt-out is in place for the aforementioned circumstances, but the type of institutions authorised to access such data are precisely defined in Recital 54:

"[…] Such overrides should only be available to health data users that are public sector bodies, or relevant Union institutions, bodies, offices or agencies, entrusted with the performance of tasks in the area of public health, or to another entity entrusted with the performance of public tasks in the area of public health or acting on behalf of or

commissioned by a public authority, […] and only where the data cannot be obtained by alternative means in a timely and effective manner. […]"

Table 3 shows a list of uses of the concept of public interest in the EHDS regulation.

Table 3. Findings of public interest in the articles of the EHDS regulation

Article	Title of article	Finding
1 (7)	Subject matter and scope	The EHDS regulation does not override existing EU or national rules that already permit public authorities, EU institutions or authorised private entities to access and further process electronic health data when this is necessary to perform a public-interest task.
19 (4)	Digital health authorities	Digital health authorities — and all their staff — must remain independent, free from conflicts of interest, and act solely in the public interest.
32 (8)	Obligations of importers	Importers must ensure that publicly accessible complaint channels exist allowing users to submit complaints and to receive any communication concerning any risk related to their health and safety or to other aspects of public interest
44 (3)	Handling of risks posed by EHR systems and of serious incidents	If a market-surveillance authority determines that an EHR system has caused harm also in terms of certain aspects of public interest protection, the manufacturer must promptly supply the affected individuals, users, and any other impacted parties
53 (1)	Purposes for which electronic health data can be processed for secondary use	HDABs release electronic health data for secondary use only when the health data user needs them for public- or occupational-health purposes—such as tackling cross-border health threats, conducting public-health surveillance, or safeguarding the quality and safety of healthcare, medicines, and medical devices
55 (5)	Health data access bodies	Health data access bodies — and all their staff — must remain free of conflicts of interest, act independently and serve the public interest
71 (4)	Right to opt out from the processing of personal electronic health data for secondary use	A health-data request is admissible when it comes from a public-health authority (or an entity acting on its behalf) and the data are needed either for the specific public-health purposes listed in Article 53(1)(a–c) or for scientific research of significant public interest, even if an opt-out exists and the data cannot be obtained by alternative means and the health data applicant has provided the justification referred to in Article 68(1)(g), or in Article 69(2)(g) to fulfil purposes of public interest in the area of legitimate scientific and societal objectives.
92 (1)	European Health Data Space Board	Members of the EHDS Board shall undertake to act in the public interest and in an independent manner.
101	Representation of a natural person	Individuals who feel their rights under the EHDS regulation have been violated may authorise a not-for-profit data-protection body having statutory public interest objectives to lodge a complaint or exercise the rights set out in Articles 21 and 81 on their behalf.

In the GDPR, the concept of public interest is used in a similar manner, as Article 6(1)(e) of the GDPR under the section titled “Lawfulness of processing”, states:

“[…] Processing shall be lawful only if and to the extent that at least one of the following applies: […] the 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.”

Furthermore, Article 9(2) of the GDPR provides examples that are identical to those found in the EHDS regulation (see references listed in Table 4). It also clarifies that the relevant protection must be ensured by the applicable Union or member state legislation in these cases:

“[…] processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or member state law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; […]”

Summarising public interest in the EHDS regulation is invoked as a 'legal justification for data processing', a 'framework for overriding consent in emergencies' and for 'assigning responsibilities to EHDS authorities', and it is consistent with the phrasing used in the GDPR.

6.3.2 General reflections

The EHDS regulation treats public interest as both an enabling principle and a normative benchmark:

- **Enabling principle.** Public-interest purposes constitute the legal gateway for secondary use: only data processing that is necessary for clearly enumerated public-health objectives or for scientific research “for important reasons of public interest” may receive access to data from an HDAB. The necessity test, together with proportionality checks in Articles 68(1)(b), 69(2)(b) and 70, ensures that public interest is weighed against data-protection obligations rather than asserted abstractly.
- **Governance standard.** Bodies charged with implementation and oversight — the national digital health authorities, HDABs and the EHDS Board — must demonstrate independence and avoid conflicts of interest precisely to safeguard public-interest decision-making. This requirement institutionalises public interest as a criterion for administrative integrity.
- **Risk-mitigation trigger.** Market obligations (importer complaint channels, manufacturer disclosure after incidents) are explicitly linked to “public-interest protection”. Thus, when a risk materialises, the duty to inform and to act is activated not only by private harm but also by broader public-interest considerations.
- **Procedural guarantee.** Individuals can rely on civil-society organisations with public-interest mandates to enforce their rights, which embeds public-interest advocacy in the enforcement architecture.

In sum, the regulation operationalises public interest through concrete conditions of access, institutional duties of independence, and responsive obligations for economic operators. Public interest is therefore not a vague aspiration but a measurable legal test that guides data-access decisions, shapes governance ethics and triggers protective measures throughout the EHDS.

The need for a more precise definition of 'public interest', particularly in relation to health research and innovation, has been emphasised. It has also been noted that there is difficulty in distinguishing projects that genuinely contribute to surveillance or safety. Examples included AI for early sepsis detection and COVID-19 impact analysis. Medicines shortages were raised as a borderline case. Concerns were expressed over subjective assessments and lack of standardisation. Furthermore, it is acknowledged that the public interest criterion under Article 53(1)(a) is vague, especially when intersecting with research and innovation projects.

Another aspect associated with the concept of public interest is 'ensuring high standards of quality and safety of health care' and its significance for scientific research and innovation. Here, too, the association can be made with the overarching goal of benefiting society. In individual cases, the degree and scope of 'high quality and safety' should be defined in as measurable terms as possible in order to facilitate assessment.

One of the main challenges with the concept of public interest is that it may be subjectively determined, making it difficult to standardise and ensure consistency as it is a broad concept which may include anything that serves a broader interest of the society. Therefore, it could be helpful for HDABs, and for increasing transparency for data applicants, if member states could provide for decision-making bodies to form part of the HDABs.

While there is no clear definition of 'public interest' there has been an ongoing discussion specific to secondary use of health data between experts about the advantages of a broad or narrow interpretation of 'public interest' and the need to identify public interest a priori.[3]

Insofar as the more legal concept of public interest is also informed by what constitutes the 'common good', this expertise regarding the definition of public interest could or even should be informed by the public themselves, including citizens and patients, as their values should guide what constitutes the common good.[4]

6.3.3 Recommendations for implementation

This provision must be interpreted in light of its public governance focus: it applies to public health authorities or bodies tasked with activities such as surveillance, monitoring, and protection of public health, not to general research or private sector development activities.

[3] Cervera De La Cruz, P., & Shabani, M. (2025). Conceptualizing fairness in the secondary use of health data for research: a scoping review. Accountability in Research, 32(3), 233–262.
[4] TEHDAS (2023). Qualitative Study to Assess Citizens' Perception of Sharing Health Data for Secondary Use and Recommendations on How to Engage Citizens in the EHDS.

- HDABs should carefully assess:
  - if the applicant is entitled to invoke this purpose (e.g. a public body with a health protection mandate, or a third party acting on its behalf), and
  - if the project or activity genuinely falls within the scope of public health interest, and not another purpose such as research (Article 53(e)).

Relevant examples could include:

- Monitoring of antimicrobial resistance,
- Using large, longitudinal, multi-institutional datasets from intensive care units (ICU) to develop an AI-based sepsis early-warning system,
- Safety tracking of advanced medical therapies,
- Assessing the impact of COVID-19 on at-risk populations,
- Post-market evaluations of cardiac medical devices.

- HDABs should by following this determination have a clear investigative responsibility or obligation to determine what type of data access is being requested and by whom and for what purpose exactly.
    - A helpful question to identify “public interest” as a purpose for the application could be: “Is the data access application comparable to the examples given above?” and “Is the applicant by affiliation or proof eligible to apply?”.
- HDABs should take into account that projects involving technology development or clinical deployment, such as AI tools for diagnosis or treatment optimisation, when answering the questions and assessing the intended purpose specified by the applicant.
    - These typically do not fall under Article 53(a) unless they are part of a recognised public health programme or legal task. These are more appropriately assessed under Article 53(e) or (f).
- The HDAB should examine both the applicant and the exact purpose, as defined in the application form.
    - The mandate, institutional role and documented objective must be examined together. Whether the activity is in the public interest depends more on the desired outcome than the type of activity.

Under Article 53(1)(a) there may be challenges in evaluating applications submitted by public bodies, particularly when access to data is needed to fulfil tasks outlined in their official mandates. In ongoing discussions, concerns have been raised about how to clearly define the roles and responsibilities of national coordination entities within public institutions. These entities may operate under their own mandates, while also engaging in coordination tasks on behalf of the national system. Furthermore, public institutions often encompass multiple roles — including data holding, regulatory responsibilities, and research — which can lead to internal conflicts or prioritisation challenges.

As a result, challenges may arise in establishing a nationally consistent and fair approach to prioritising such applications. There may be a need for the development of standardised procedures or guidelines to ensure transparent and effective handling of these complex cases through all member states.

6.4 Article 53(1)(b) – Policymaking and regulatory activities

Article 53(1)(b) refers to the term ‘policymaking and regulatory activities’ as follows:

"[…] policymaking and regulatory activities to support public sector bodies or Union institutions, bodies, offices or agencies including regulatory authorities, in the health or care sector to carry out their tasks defined in their mandates; […]"

The aspects of policymaking and regulatory activities are not frequently addressed in the EHDS articles but are mentioned in the recitals:

- Recital 6 states that the fact that electronic health data may also be collected and processed for policymaking or regulatory purposes and should be made available in accordance with the EHDS regulation.
- Recital 110 positions policymaking and regulatory activities as a core 'public interest' goal of the EHDS regulation.

6.4.1 General reflections

Article 53(1)(b) can be understood in conjunction with Recitals 6 and 110 as one of the essential objectives of the EHDS. National coordination measures alone have proved insufficient — an insight drawn from the evaluation of Directive 2011/24/EU. Because policymakers and regulators need comparable, cross-border evidence, the text of Recital 110 argues that only harmonised Union rules can secure consistent access to electronic health data. This satisfies the principle of subsidiarity: Union intervention is justified when objectives cannot be met effectively by member states acting separately.

The regulation will create common rights, interoperability requirements and safeguards for primary and secondary use of data. These harmonising measures give policymakers and regulators a stable legal and technical environment in which to obtain and reuse health data. The result is an enabling infrastructure for data-driven legislation, standard-setting, market surveillance and public-health planning.

By invoking the principle of proportionality, Recital 110 affirms that the regulation introduces no greater obligations than necessary. In regulatory terms, this signals a calibrated approach: it balances individual data-protection rights with the informational needs of competent authorities, thereby fostering "regulatory flexibility" while still guarding fundamental rights.

6.4.2 Recommendations for implementation

- HDABs should develop mechanisms to enable the prioritisation of tasks, if there is sufficient justification for doing so.
- HDABs should retain the ability to ask clarifying questions in order to determine the specific role and intended outcome/purpose of the data applicant's request for health data.
- HDABs should not “prioritise tasks” unless explicitly mandated to do so. Their role is to assess eligibility under Article 53(1)(b), not to allocate priority across policy domains.
    - If multiple applications meet the requirements under Article 53(1)(b), Member States may consider establishing mechanisms to guide prioritisation, where justified by public-health imperatives.

6.5 Article 53(1)(c) – Statistics

The ‘statistics’ referred to in Article 53(1)(c) as a purpose of secondary use are very specifically limited and defined here; they refer to (inter)national statistical bodies, which are usually part of the institutional health care system:

“[…] statistics as defined in Article 3(1), of Regulation (EC) No 223/2009[5], such as national, multi-national and Union-level official statistics, related to health or care sectors; […]”

Article 3(1) of regulation (EC), No 223/2009 mentioned above, defines statistics as “quantitative and qualitative, aggregated and representative information characterising a collective phenomenon in a given population”.

Consequently, the term encompasses official statistical outputs that have undergone anonymisation and aggregation, thereby ensuring the description of groups rather than identifiable persons.

The term 'statistic' is supplemented with various additional aspects in the recitals and in Article 2 of the EHDS regulation:

- Recital 1: Lists “official statistics” among the societal purposes of secondary use.
- Recital 56: Notes that secondary-use data can include sets initially collected for statistics and other public-interest tasks.
- Recital 87: Calls for harmonised templates for registries and datasets, explicitly mentioning statistics as an area where standardisation work is advanced.

[5] The European Statistical System (ESS) is the institutional network that produces and disseminates European official statistics. It comprises Eurostat, the national statistical institutes of all EU Member States, other national authorities that compile statistics, and the statistical services of EEA–EFTA countries, see https://ec.europa.eu/eurostat/web/european-statistical-system.

- Article 2(2)(t): Counts organisations that process data for official statistics among the "health data holders" obliged to make data available.

6.5.1 General reflections

The defining characteristic of statistics, particularly national statistics, is not a specific quality or single use, but rather its broad and general purpose. National statistics function as part of an information infrastructure designed for widespread and varied use. They are not produced for a narrowly defined occasion or tailored to a specific user need. Instead, they consist of tabulations, calculated indicators, and other outputs intended to serve multiple purposes across many sectors.

Taken together, these provisions show that Article 53(1)(c) is confined to national, multi-national and EU-level official statistics produced under the European statistical system (ESS)[6]. The data concerned are:

- **Aggregated and representative** – they summarise phenomena at population level.
- **Anonymised/confidential** – micro-data remain protected under statistical-confidentiality rules in Regulation 223/2009[7].
- **Health-or care-related** – only statistics that describe health status, healthcare utilisation, health workforce, expenditure, etc., fall within the scope.

Since all analyses use statistics, this precise and strict definition is particularly important here, as it means that this purpose may only be used by public bodies. Entities not already subject to existing obligations to report data may still be involved in providing information for the production of statistics that extend beyond such obligations.

From a technical standpoint, it is generally clear what constitutes statistical data. However, the intended use of such data is often less straightforward.

The wording of the article implies that other types of public bodies that are not formally designated as statistical bodies. only entities legally mandated to produce official statistics under national or EU law can invoke Article 53(1)(c). Other public bodies conducting analytical work should apply under Article 53(1)(b) or (e).

6.5.2 Recommendations for implementation

These uncertainties make it difficult to assess the full scope of purpose 53(1)(c). While an application clearly referencing statistics may be understandable in its intent, it remains

[6] The European Statistical System (ESS) is the institutional network that produces and disseminates European official statistics. It comprises Eurostat, the national statistical institutes of all EU Member States, other national authorities that compile statistics, and the statistical services of EEA–EFTA countries, see https://ec.europa.eu/eurostat/web/european-statistical-system.

[7] REGULATION (EC) No 223/2009 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 March 2009 on European statistics and repealing Regulation https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009R0223

unclear who is authorised to apply under this purpose, and from which point in time — especially in relation to existing legal provisions and institutional roles.

Is purpose (c) intended to cover activities already established by law, or does it extend to additional or complementary statistical uses? Furthermore, does it allow non-designated public sector bodies to engage in statistical analyses for this purpose? It should be clarified that Article 53(1)(c) does not extend to general analytical or research uses, even by public authorities, unless they are acting within a recognised statistical mandate.

These questions have implications for the data catalogue, particularly for smaller health data holders, as they might not be prepared for the responsibilities or consequences associated with providing data for statistical purposes under purpose 53(1)(c).

If an authority is explicitly mandated to produce national statistics and seeks to use data for this purpose, such use can be considered legitimate within the framework of purpose (c), provided that the statistical processing aligns with the definition under Regulation (EC) No 223/2009 and that the applicant's institutional role is clearly documented.

- HDABs should have the ability to ask clarifying questions to determine the capacity in which the applicant is requesting access to the data. Recital 162 of the GDPR provides further relevant context for interpreting the notion of statistics

6.6 Article 53(1)(d) – Education

Under Article 53(1)(d), access to health data is allowed for "[…] education or teaching activities in health or care sectors at vocational or higher education level; […]".

6.6.1 General reflections

This guideline does not cover educational activities that fall outside the scope of vocational or higher education, as only these are eligible under Article 53(1)(d). When considering educational activities under purpose (d), the focus should be on whether the activity involves training that necessitates access to sensitive health data on an individual level. This applies regardless of the underlying reason — whether legal, technological (AI), or otherwise. If such access is required to support the educational objectives, then purpose (d) should be a relevant reason for data access.

This provision refers to the purpose of the activity, rather than the status of the applicant. 'Health and care sectors' are wider than 'medicine' only. It is part of a formal educational or training activity relevant to the health or care sectors (e.g. medicine, nursing, pharmacy, biomedical informatics, public health, or social care).

It aims to support learning objectives or practical teaching (e.g. simulated case studies, classroom exercises) as well as improving healthcare professional training.

Regarding the classification of an application under this purpose, there will be some overlap with purpose (e), 'scientific research'.

Digital health tool training, for instance, includes wellness applications, AI training, and similar activities. However, training that involves tool development, evaluation, or general digital health literacy may not qualify under Article 53(1)(d) unless it is part of a formal curriculum. Instead, research and testing activities are more appropriately assigned to purpose (e), as they suggest rigorous testing of the application, including ethical review.

Therefore, HDABs should check which purpose best describes the issue. Contacting the applicant is also particularly important in this regard to make sure that the educational purpose is clearly stated in the application and supported by documentation such as course descriptions or training programme outlines.

It is crucial to be aware that, as clarified in Recital 52 of the EHDS regulation, this regulation does not affect the initial processing of electronic health data by health data holders, such as for the delivery of healthcare. These activities do not involve making data available to others. Such uses, which fall within the original purpose for which the data were collected, remain outside the scope of the EHDS framework for secondary use and are not subject to data permit requirements. They may therefore continue in accordance with applicable data protection legislation, including the GDPR.

6.6.2 Recommendations for implementations

- HDABs should distinguish education/training from scientific research. For instance, the use of health data in the context of a thesis or dissertation (e.g. Master or PhD project) may fall under either:
  - Article 53(1)(d), if the primary goal is educational (learning/training); and/or
  - Article 53(e), if the primary goal is scientific knowledge production or publication.
- In some member states, for example, a master's thesis is not considered to be scientific research, but rather an educational exercise.
- HDABs should assess the declared objective, supervision context, and methodology accordingly.
  - In practice, there would be concerns of a non-insignificant nature, such as data protection safeguards, confidentiality/secrecy issues, and ethical approval.

While the EHDS regulation does not require the applicant to be an educational institution or educator, the involvement of a recognised programme or supervisor may help demonstrate the legitimacy and structure of the educational purpose.

6.7 Article 53(1)(e) – Scientific research

Under Article 53(1)(e) access to health data is allowed for scientific research purposes. The interpretation of this is meant broadly (aligning with the use of 'scientific research' in GDPR Recital 159), which is indicated by a non-exhaustive list of examples, such as development and innovation activities for products or AI development and algorithm training. Data uses that are applied for under this purpose must genuinely qualify as scientific research and show this by providing verifiable documentation (e.g. scientific protocol, funding source, academic supervision). Projects driven without a clear scientific aim and without scientific methods do not qualify.

Furthermore, the scientific research under the meaning of Article 53(1)(e) shall contribute to public health or health technology, assessments, or ensure high levels of quality and safety of healthcare, of medicinal products or of medical devices, with the aim of benefiting end-users, such as patients, health professionals and health administrators.

6.7.1 The concept of "scientific research"

Scientific research is not defined in any legal act, not even in the GDPR, although the concept appears in many different contexts, such as in the aforementioned legislation.

Scientific research is a heterogeneous activity, that encompasses a wide variety of methods, theories, and disciplines, and is a socially embedded practice that is shaped by institutional norms, funding structures, and political contexts.[8] Scientific research is usually characterised by a systematic approach, empirical grounding, transparency, and ethical conduct. It often begins with a clear research question or problem, aims to contribute to existing body of knowledge in a particular field, and may be theoretical or applied in nature. Research findings are typically subject to peer review by experts in the field and/or published in academic journals or presented at conferences.

As indicated by Recital 159 of the GDPR, "the term processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research including privately funded research. In addition, it should consider the Union's objective under Article 179(1) TFEU of achieving a European Research Area. Scientific research purposes should also include studies conducted in the public interest in the area of public health".[9]

Recital 61 of the EHDS regulation indicates an almost verbatim explanation of the concept: "The notion of scientific research purposes should be interpreted in a broad manner, including

[8] Knorr-Cetina, Karin (1981). The manufacture of knowledge: an essay on the constructivist and contextual nature of science. New York: Pergamon Press.
[9] See Guidelines 03/2020 of the EDPB from 21.4.2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, pages 5–6.

technological development and demonstration, fundamental research, applied research and privately funded research."

It also states: "Activities related to scientific research include innovation activities such as training of AI algorithms that could be used in healthcare or the care of natural persons, as well as the evaluation and further development of existing algorithms and products for such purposes."

The Working Party for the former Article 29 has pointed out that "the notion may not be stretched beyond its common meaning and understands that "scientific research" in this context means a research project set up in accordance with relevant sector-related methodological and ethical standards, in conformity with good practice."[10]

Article 53(1)(e) allows access to health data for scientific research purposes and includes specific examples such as AI development and algorithm training, research conducted by public and private actors or applied or innovation-oriented research.

These examples are introduced by the word "including", which under EU legal drafting conventions indicates a non-exhaustive list. The purpose is to clarify that such activities can fall within the concept of scientific research, without limiting it to those cases.

Therefore, the inclusion of AI and algorithm training is meant to:

- Confirm that these emerging activities can qualify as scientific research.
- Prevent narrow interpretations that might exclude applied or technology-driven research.

Ensure alignment with the broad interpretation of "scientific research" used in other EU laws, particularly the GDPR Recital 159, which explicitly recognises a wide range of actors and objectives under research.

The listed examples serve to clarify and broaden the interpretation of 'scientific research'. Therefore, it is not sufficient that the health data user is a scientific actor (e.g. from academia), or that the purpose is a typical scientific one. To allow for the broad interpretation, the relevant criterion is that any research under this provision must genuinely qualify as scientific.

The fact that the final version of the EHDS regulation no longer treats AI as a separate purpose means that data for AI development and algorithm training is only permitted when it falls within the scope of scientific research. Therefore, it does not mean that all AI-related activities are automatically permitted under Article 53(1)(e). Projects driven without a scientific aim do not qualify.

[10] See Guidelines on Consent under Regulation 2016/679 of the former Article 29 Working-Party from 10.04.2018, WP259 rev.01, 17EN, page 27 (endorsed by the EDPB). Available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

6.7.2 The concept of "innovation activities"

Regarding the concept of innovation, Recital 31 of Regulation (EU) 2021/695[11] states i.a. "[…] the concept of innovation should be used in accordance with the Oslo Manual developed by the OECD and Eurostat, which follows a broad approach that covers social innovation and design."

According to the Oslo Manual[12] "A business innovation is a new or improved product or business process (or combination thereof) that differs significantly from the firm's previous products or business processes and that has been introduced on the market or brought into use by the firm".

In the glossary of the European Statistical Office (Eurostat) innovation is the use of new ideas, products or methods where they have not been used before.[13]

6.7.3 General reflections

- Both applied and basic research are included in purpose (e), and do not necessarily have direct benefits to end-users or patients but rather unfold their societal benefits over a longer run (see Recital 61).
- Data for AI development and algorithm training is only allowed when it falls within the scope of scientific research, since it is not its own separate purpose.
- Projects involving innovation activities can be eligible under purpose (e) as long as the project is based on scientific methods with clear hypotheses, or public interest aims. Commercial interest does not disqualify a project per se, but scientific rigor must be demonstrated (e.g. research protocol, peer review publication plan etc.).
- Research regarding fields, that might not be thought of as health or care sector related (e.g. cosmetic surgery with no medical indication), falls within purpose (e) if the aim of the research is related to health or care sectors and contributes to public health or health technology assessments, or ensures high levels of quality and safety of healthcare, of medicinal products or of medical devices, with the aim of benefiting end-users, such as patients, health professionals and health administrators. A concrete example would be to increase the safety of cosmetic surgery.
- Studies of the development of products that are not medical devices within the meaning of the Medical Device Regulation (MDR) or in vitro diagnostic regulation fall under purpose (e), as long as the research is intended to benefit patients. Such

[11] Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/2013
[12] OECD/Eurostat (2018), Oslo Manual 2018: Guidelines for Collecting, Reporting and Using Data on Innovation, 4th Edition, The Measurement of Scientific, Technological and Innovation Activities, OECD Publishing, Paris/Eurostat, Luxembourg, page 68.
[13] OECD/Eurostat (2018), Oslo Manual 2018: Guidelines for Collecting, Reporting and Using Data on Innovation, 4th Edition, The Measurement of Scientific, Technological and Innovation Activities, OECD Publishing, Paris/Eurostat, Luxembourg. https://doi.org/10.1787/9789264304604-en.

products may include hospital operation and management systems using artificial intelligence, wellness or other digital health applications.

There is still a degree of uncertainty concerning what constitutes “scientific research” and which activities do not fall under this category, especially regarding who uses the data and for what the data are used. An example on the edge might be a project focused primarily on training an existing artificial intelligence system with minimal research that would gain or verify any new knowledge. However, the project must rely on a scientific basis to be eligible for purpose (e). If the intended data use falls under “scientific research”, this should not just be based on a self-determined check box. HDABs should assess the scope, methodology and aims of the project against the stated purpose. If needed the HDAB may use external scientific advisory boards to facilitate this assessment. It is unclear in how far the scope, method, and intent of a study or research can be assessed without being guided by the aspect of quality of research.

6.7.4 Recommendations

- The HDABs should retain their ability to ask clarifying questions in order to determine the specific role and intended outcome/purpose of the data applicant's request for health data.
- HDABs should check the obligatory additional verifiable documentation provided by the applicant for chosen purpose e (e.g. research plan, funding, ethics approval if needed).
- HDABs should specifically check the description of the aim, the described methods and the expected benefits when assessing if the purpose (e) is applicable.
    - These parts of the application should give the HDAB a picture of what evidence the applicant want to create to contribute to public health or health technology assessments, or ensure high levels of quality and safety of healthcare.
- HDABs is strongly recommended to have access to adequate expertise in various scientific methods and study design/protocols to provide advice in assessment of applications involving new data uses or application of methods. If needed assign advisory board(s) to provide current and valid knowledge on accepted scientific protocols etc.

6.8 Article 53(1)(f) – Improvement of healthcare

Under Article 53(1)(f) access to health data is allowed for the improvement of delivery of care, of the optimisation of treatment and of the provision of healthcare, based on data from other individuals.

This provision includes:

- Personalised medicine, where treatments are tailored based on insights drawn from broader population-level data;
- System-level improvements, such as optimising workflows, resource planning, or evaluating care models.

Both categories are within scope, provided that the data use is aimed at improving care and the project is grounded in a credible methodology.[14]

While any applicants can apply for data under purpose (f), they need to show that the purpose for the application aims not at general innovation, but at targeted care improvement. This can for example be shown by the applicant themselves being or having a direct link to a healthcare provider or public health authority, by providing proof that project outputs will be directly integrated into care pathways, or by involvement of clinical staff in the study or implementation phase. If an applicant has no link to a healthcare provider, then the direct clinical utility has to be sufficiently documented in the application for the data use to fall under purpose (f).

Examples for clarification

A clinician orders data with the aim to improve the treatment of an individual patient with a very rare disease. The clinician wants to gather data from databases across Europe to find out if there are similar cases/images/reports. This would fall under (f).

If the head of a clinic wants to compare the treatment outcomes at their clinic to the outcomes of similar patients at other clinics, hoping to learn from these comparisons and the goal of this data use is to improve their own clinic's delivery of care, with no research protocol and no intention of publishing an article in a scientific journal, then this would fall under purpose (f) and not (e).

The applicant has a prognostic tool that was developed using data that the applicant got access to under (e), the development falls under scientific research. Then when the applicant has rolled out the product, under purpose (f), the applicant can apply for data to update the product´s prognostic factor. The applicant can do so by using the latest available data from other patients, the data available in the health care system, if the goal of the update is to improve healthcare delivery. It is not allowed for product development or commercial purposes.

[14] Answers from DG SANTE, dated 16.5.2025 to WP 5, task 5.2.1.

6.8.1 Recommendations

- HDABs should verify whether the project is methodologically credible and whether the intended data use is plausibly and directly aimed at improving healthcare delivery, treatment optimisation, or care provision, in line with Article 53(1)(f).
- HDABs should check the applicant´s affiliation. While the EHDS regulation does not require the applicant to be a clinician or hospital, plausibility could be indicated by an involvement of the applicant in healthcare delivery or planning.

7 Prohibited secondary use of health data under Article 54

In this section, an analysis and recommendations are given on what to consider in the assessment process regarding the provisions on prohibited secondary use of health data under Article 54 in the EHDS regulation. The recommendations in this section are intended to complement the general recommendations set out in Chapter 6.

According to Article 54, health data users shall only access electronic health data for secondary use on the basis of and in accordance with the purposes contained in an issued data permit or approved data request, or from the relevant authorised participant in HealthData@EU referred to in Article 75. In particular, seeking access to and processing of electronic health data obtained via an issued data permit or an approved health data request for the uses mentioned in Article 54 (a–e) shall be prohibited. The prohibitions will be further discussed and analysed in the subsections below.

HDABs should monitor and supervise compliance by health data users and health data holders with the requirements laid down in the EHDS regulation (Article 57(1)(a)(ii)). Where an HDAB finds that a health data user or health data holder does not comply with the requirements (for example by violating Article 54), the HDAB should, amongst others, immediately take appropriate measures. For example, HDABs are empowered to impose administrative fines to a health data user processing electronic health data obtained via a data permit for the uses referred to in Article 54 (Article 63(2) and 64(5)(a)). See further forthcoming deliverable in TEHDAS2, D4.2.1 and D4.2.2.

7.1 Article 54(a–b) – Decisions detrimental to individuals or groups and disadvantaging or discriminating decisions

Article 54 states that in particular, seeking access to and processing electronic health data obtained via a data permit issued pursuant to Article 68 or a health data request approved pursuant to Article 69 for the following uses shall be prohibited:

a) taking decisions detrimental to a natural person or a group of natural persons based on their electronic health data; in order to qualify as ‘decisions’ for the purposes of this point, they have to produce legal, social or economic effects or similarly significantly affect those natural persons;

b) taking decisions in relation to a natural person or a group of natural persons in relation to job offers, offering less favourable terms in the provision of goods or services, including exclusion of such persons or groups from the benefit of an insurance or credit contract, the modification of their contributions and insurance premiums or conditions of loans, or taking any other decisions in relation to a natural person or a group of natural persons which result in discriminating against them on the basis of the health data obtained.

According to Recital 62, any attempt to use electronic health data for measures detrimental to natural persons, such as to increase insurance premiums, to engage in activities potentially detrimental to natural persons related to employment, pensions or banking, including mortgaging of properties, to advertise products or treatments, to automate individual

decision-making, to re-identify natural persons or to develop harmful products, should be prohibited.

7.1.1 The concept of "discrimination"

The EHDS regulation does not say that Article 54(b) targets discrimination under Union law (compare for example the wording in Article 10.2 (f) in the AI Act).[15] However, due to the context in which the concept is used, task 5.2.1 consider that it is the most reasonable way to understand it.

It is a fundamental right not to be discriminated against. Article 21 in the EU Charter of Fundamental Rights (hereinafter "the Charter") states that any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited. Further, within the scope of application of the Treaties and without prejudice to any of their specific provisions, any discrimination on grounds of nationality shall be prohibited. Operational indicators that HDABs could pay attention to are for example use of data to segment individuals by health status in pricing models, service offers, or recruitment filters.

The provisions of the Charter are addressed to (i) the institutions and bodies of the EU directive in all their actions, national authorities when they are implementing EU law, and (ii) national authorities when they are implementing EU law. For example, the Charter applies when EU countries adopt or apply a national law implementing an EU directive[16] or when their authorities apply an EU regulation directly.[17]

7.1.2 General reflections

It might be difficult for an HDAB to figure out if a health data user is seeking access to and will process electronic health data for a prohibited secondary use under Article 54(a) or 54(b). In most cases it will not be stated in the application. Instead, an infringement might be discovered as a result of an HDABs monitoring compliance under Article 57(1)(a)(ii)) or indications from an external part (for example from the public or media). By then, the harm for the affected individuals or groups is already done. In order to try to prevent such a situation, HDABs should require applicants to provide a binding declaration that the data will not be used for prohibited purposes under Article 54(a–b), including profiling, scoring or automated decision-making, that leads to exclusion or discrimination.

All kinds of decision-making, both "ordinary" (no machine involved), semi-automated and automated decision-making, are covered by Article 54(a–b). The emphasis is on the impact of the decision on the data subject. To be able to assess if a secondary use of electronic health data is contrary to the prohibition in Article 54(a) or 54(b), HDABs must have adequate competence or have access to relevant support for the task (for example technical and legal support, including competence on data protection under GDPR).

[15] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024.
[16] Directives set binding objectives upon EU member states to achieve a certain result but leave them free to choose how to achieve these objectives.
[17] Applying the EU Charter of Fundamental Rights (25 April 2025).

The Commission has clarified that although parallels can be drawn with Article 22 of the GDPR, the scope of Article 54(a) of the EHDS regulation is broader. It prohibits the processing of electronic health data for any decisions detrimental to individuals or groups — whether automated, semi-automated, or manual — and is not limited to specific categories of personal data. These decisions may include, for example, exclusion from services or unfair prioritisation. HDABs should therefore not assume that compliance with GDPR Article 22 is sufficient to ensure compliance with Article 54(a). Further operational clarification could be developed by the EHDS Board, as referred to in Recital 95.

7.1.3 Recommendations

- HDABs should put emphasis on the impact of the decision on the data subject. Therefore, HDABs should assess whether the stated use case suggests such risks.
- HDABs should make sure that applicants provide enough details to rule out that the data use will feed into a harmful or discriminatory decision-making process.
- HDABs should assess whether the described data use could plausibly result in decisions that significantly affect individuals or groups. For instance, HDABs may pay attention to who the applicant is, what types of decisions the project entails and whether exclusionary impacts are foreseeable.
- Examples of red flags are:
  - Risk-scoring tools with individual-level consequences (for example exclusion from services, automated triage systems).
  - Automated profiling for eligibility in health insurance or access to services.
  - AI systems that produce binding clinical decisions without human oversight

7.2 Article 54(c) – Marketing activities

Under Article 54(c) it is prohibited to seek access to and process electronic health data for the use carrying out advertising or marketing activities. In Recital 62 the legislator´s intentions are stated and amongst others, it can be read that any attempt to use electronic health data to advertise products should be prohibited. The prohibited use does not only include

marketing or advertising activities towards health professionals, organisations in health or natural person but all possible target audiences which marks a shift from the proposal.[18]

Marketing is overall strategy and process of identifying customer needs and promoting products or services to meet those needs. It includes, amongst others, market research, product development, pricing, distribution, branding, and customer engagement. Advertising is a subset of marketing. In Article 2(a) of Directive 2006/114/EC, advertising is defined as "the making of a representation in any form in connection with a trade, business, craft or profession in order to promote the supply of goods or services, including immovable property, rights and obligations". It refers specifically to the promotion of products, services or ideas through various channels with the goal of influencing consumer behaviour.[19]

7.2.1 General reflections

Marketing activities, especially when based on patient preferences, diagnosis history or behavioural data, even when anonymised, can undermine public trust and conflict with the GDPR principle of purpose limitation. A common risk scenario involves pharmaceutical companies using health data not for legitimate research or innovation, but for targeted marketing or pricing strategies.

For instance, a pharmaceutical company would not be allowed to request data on medications (e.g. ATC codes) prescribed by doctors in all hospitals within a specific ICD-10 category, with the intent of launching targeted marketing campaigns in hospitals where the prescription rate of a particular medication is low.

It is crucial to distinguish between permitted use, such as scientific research and prohibited use, such as marketing studies. As outlined above in the chapter 7.7.1 and in EHDS Recital 61 the notion of scientific research purposes should be interpreted broadly, including both privately and publicly funded projects. One of the core goals of the EHDS regulation is to enable innovations that benefit society. While research is essential, it is also important that research outcomes lead to practical applications, which may take the form of commercial products or services. The Recital 61 states the secondary use of health data for research and development purposes should contribute to benefiting society in the form of new medicines, medical devices, and healthcare products and services at affordable and fair prices for Union citizens, as well as to enhancing access to and the availability of such products and services in all member states. While both permitted and prohibited use can share a key motivator (commercial gain) the distinction in regulatory context is how the data is used and for what immediate purpose. Outcome of scientific research may be a commercial product if the data use itself is not promotional. Similarly, marketing-related studies aimed at segmenting consumers or testing product messaging do not qualify as scientific research under Article 53(e), even if they use research-like methods. The actual purpose, not the methodology or eventual profit, defines the legal basis. These distinctions must be clearly maintained. Evaluating the purpose, focus, timing, and how the data are used

[18] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Health Data Space COM/2022/197 final, Article 35(c).
[19] Directive 2006/114/EC of the European Parliament and of the Council of 12 December 2006 concerning misleading and comparative advertising (codified version).

can help the HDAB to determine whether the intended use is permitted or prohibited. Ultimately, the health data user bears the final responsibility for ensuring compliance.

Questions arise in cases where health data are initially requested for a legitimate purpose but is later used for marketing that product. HDABs should be mindful that commercial actors may have mixed motives. Where the project's aims, context or documentation raise doubts about whether data might be used to promotes specific products or services, further scrutiny is warranted. A company may submit a data request with a legitimate aim, but the eventual use of the data may diverge from that purpose.

It is essential to ensure that applicants focus on and act in accordance with allowed purposes under Article 53 and don´t cause harm under Article 54. Still, monitoring the long-term outcomes of health data use remains a significant challenge.

7.2.2 Recommendations

- HDABs should carefully assess whether the intended data use could directly or indirectly support advertising or marketing activities.
    - Special attention should be paid to applications from commercial actors whose business models include, i.e., sales, promotion, or segmentation of customers.
    - The applicant's background should be considered.
    - If the applicant's business model, prior use cases, or vague purpose raise concerns, the HDAB may seek clarification or deny the permit.
    - Risk factors include vague project objectives, absence of a scientific protocol, or reference to market testing, product positioning, or consumer insights. Where such risks exist, HDABs should request clarification or, where appropriate, deny the request under Article 54(c).
    - Applicants should be reminded that re-use of data for advertising purposes is strictly prohibited, regardless of the original purpose
    - A clear distinction between permitted research or innovation under Article 53(e) and prohibited marketing activities under Article 54(c) needs to be done by the HDAB. Evaluate the purpose, focus, timing and the way data will be used.

7.3 Article 54(d) – Developing harmful product or service

Under Article 54(d) it is prohibited to seek access to and process electronic health data for the use developing products or services that may harm individuals, public health or society at large, such as illicit drugs, alcoholic beverages, tobacco and nicotine products, weaponry or products or services which are designed or modified in such a way that they create addiction, contravene public order or cause a risk for human health. These examples are introduced by the word "such as", which under EU legal drafting conventions indicates a non-exhaustive list concluding that the definition of a "harmful product" is contextual and purpose-driven. Recital 62 states that any attempt to use electronic health data to develop harmful products should be prohibited.

Situations may occur where the declared purpose under Article 53 appears legitimate, but the potential downstream may conflict with Article 54(d). Under Article 68(1)(a-b), HDABs shall assess whether the purpose is specific, proportionate and consistent with the applicant's profile. For example, if a tobacco company applies to study the health impacts of smoking, HDABs must evaluate whether the data could be repurposed to develop addictive products, which would be prohibited.

7.3.1 General reflections

HDABs should scrutinize applications for clarity and consistency and request further documentation or clarification when necessary. When residual uncertainty persists, HDABs should apply a precautionary approach. The declared purpose must be specific and consistent with the applicant's profile, and any potential downstream use that contradicts Article 54(d) should prompt further scrutiny. The primary focus should be on ensuring that the permitted use does not result in harm.

In most cases, prohibited purposes are unlikely to be explicitly stated in the application. Therefore, it is recommended that permits must clearly specify that the data are granted for specific use only, and that this use cannot be altered. This requirement should be explicitly reflected in the data permit, in line with Article 68(1)(a), to ensure that only the approved use is permitted, and that any deviation would constitute a breach. Nonetheless, concerns remain about whether simply stating the purpose and including a summary from the applicant is sufficient to prevent misuse.

The line between permitted and prohibited use may become blurred if the data could also be used to "improve" the company's products, potentially making them less harmful, yet still addictive or risky to the public health. For example, making tobacco less carcinogenic but still containing carcinogenic substances that are addictive and deadly or products to replace tobacco with other less harmful yet similarly addictive products. This raises the question of how an HDAB should evaluate such a case, and whether the intended use is permissible or entails a risk of prohibited misuse.

Another example includes the use of health data to study narcotics for the development of new medicines. Article 54(d) of the EHDS regulation prohibits secondary use of data for developing illicit drugs, but EHDS does not define what constitutes an "illicit drug". While

legislation such as directive (EU) 2017/2103[20] provides definitions, the lists are non-exhaustive, and definitions may vary between member states. Moreover, the classification of narcotics evolves over time and includes a wide range of central nervous system-active substances, many of which were not originally developed as narcotics but have since been misused. Several of these substances are also used in regulated medical contexts, such as in the treatment of ADHD. This raises the question of whether HDABs should deny permits in all such cases, or whether research into these substances should be allowed when the goal is to develop safer or more effective treatments. These situations require extreme caution and clarity.

Commercial applicants may submit legitimate requests, but HDABs must assess whether the intended use aligns with Article 53 and does not risk violate Article 54(d). In cases of concern, HDABs should conduct a detailed review and, where necessary, consult legal experts or data protection officers to ensure compliance.

7.3.2 Recommendations

- HDABs should assess whether the project, even if framed under an allowed purpose, may result in outcomes that fall under Article 54(d) (e.g. reinforcing addictive behaviours, optimising harmful consumption).
- HDABs should scrutinise both the declared objective and foreseeable downstream uses, when the applicant operates in a sensitive sector (e.g., tobacco, alcohol, gambling).
- HDABs should, when risks are unclear, be encouraged to consult legal or ethical experts, or refer to national guidelines, before issuing a permit.
- HDABs may not have formal powers to enforce long-term monitoring. Therefore, member states should consider including, in national guidelines or through HealthData@EU, good practices for post-permit transparency (e.g., voluntary publication linkage), while recognising that.

7.4 Article 54(e) – Ethical provisions under national law

Under Article 54(e) and Recital 62, it is prohibited to seek access to and process electronic health data for purposes that conflict with ethical provisions laid down in national law. With the exception of ethical provisions relating to consent to the processing of personal data and

[20] Directive (EU) 2017/2103 of the European Parliament and of the Council of 15 November 2017 amending Council Framework Decision 2004/757/JHA in order to include new psychoactive substances in the definition of 'drug' and repealing Council Decision 2005/387/JHA.

provisions relating to the right to opt out since the EHDS regulation takes precedence over the national law.

Before granting access to electronic health data, the HDAB must assess whether all applicable criteria are met. As part of the application, the applicant shall give information on any assessment of ethical aspects of the processing required under national law, which may serve to replace the health data applicant's own ethical assessment (Article 67(2)(j)). The HDAB must then assess whether this information complies with national law before issuing a data permit (Article 68(1)(f)).

For further guidance, see the Guideline for data users on good application and access practice (T6.2) and Guideline for HDABs on the procedures and formats for data access (T6.3).

The legislator´s intentions are stated in Recital 73: An ethical assessment could be requested based on national law. In that case, it should be possible for existing ethics bodies to carry out such assessments for the HDAB. Existing ethics bodies of member states should make their expertise available to the HDABs for that purpose. Alternatively, member states should be able to organise the structure of the HDAB to include specialises on ethics or have a close collaboration with ethics bodies.

Further, in Recital 83, it says that the authorisation process to gain access to personal electronic health data in different member states can be repetitive and complex for health data users. Whenever possible, synergies should be established to reduce the burden and barriers for health data users. One way to achieve that aim is to adhere to the 'single application' principle whereby, with one application, the health data user can obtain authorisation from multiple HDABs in different member states or authorised participants in HealthData@EU.

7.4.1 General reflections

When it comes to ethical provisions in national legislation, the legislation may look different in different member states. Currently, in the EU there are varying practices and standards in how ethical review process is organised at national level. So far, it has not been defined how the support to the HDABs should be organised across the member states, in order to tackle juridical or ethical problems.

In general, among the member states, there is a uniform understanding that medical research or studies involving invasive clinical testing, require ethical approval from a medical ethics body. However, among the member states there is a varied recognition or already set up system for seeking ethical approval for non-medical research, for example survey studies, which deals with sensitive questions or use of data (such as rare diseases, or sensitive personal data, or data on specific population groups that may be stigmatising or unethical outcomes). Existence of an ethics body which also deals with non-medical studies within the member states may vary from country to country.

Currently there is a great variation in the national legislation concerning ethical review process in the member states. In Sweden medical research must be ethically reviewed and approved by the Swedish Ethics Review Authority. That means that the health data users need to have applied for ethical approvals prior to applying for health data. This cannot be

replaced by the applicants' own ethical assessment of their work. In Finland, the need for ethical review is also recognised. Medical ethics review boards are linked to regional hospitals and are hospital-district specific. Furthermore, there are also numerous non-medical ethics boards which aim to provide ethical review on questions which are not regarded as medical, but are sensitive in nature, for example studies on underage children, studies involving questionnaires where sensitive data are collected etc. In any case, whether required by the national law or not, an ethical assessment of some sort is a natural part of the application evaluation process and should not be left out completely.

As outlined in Article 55(2), member states are required to ensure that each HDAB is provided with adequate human, financial, and technical resources, along with the necessary expertise, premises, and infrastructure. This should include ensuring structured access to ethics bodies or advisory services.

Such access facilitates accurate guidance on whether an ethical review is legally required by the national law and ensures that, when HDABs conduct ethical assessments not mandated by national law, these reviews are carried out in a more professional, consistent, and credible manner. It is particularly valuable in cases where the legal requirements for ethical review are unclear, where a review is not legally required but ethical aspects must still be considered, or where applicant-provided self-assessments are biased or of varying quality.

Ethical provisions under national law remain diverse across the EU. Where national legislation requires an ethical review of secondary use applications, HDABs must ensure that such requirements are fulfilled. Member states are responsible for defining the applicable ethical rules and for equipping HDABs with the necessary resources and cooperation mechanisms — such as access to national ethics bodies or expert support. The EHDS regulation does not establish a harmonised EU-level ethics system, but it does require that national ethical requirements be respected in the context of secondary use assessments.

7.4.2 Recommendations

- HDABs should have an ethical assessment included in their assessment process, even though the EHDS does not specifically require one. When the national law does not require an ethics review the HDAB should still evaluate the applicant's own ethics assessment, is it sound and does it raise any concerns. In the absence of such the HDAB should do the assessment. Thus, just checking whether a self-assessment has been made is not enough.
- HDABs should be able to access legal and ethical advice where needed, especially in cases where national law requires an ethical assessment or where the application raises complex ethical concerns.
- Member states are encouraged to provide structured access to ethics bodies or advisory services to support both applicants and HDABs, especially in cases involving complex or non-medical studies.
- HDABs should ensure that clear, accessible information on national ethical assessment requirements is available to applicants, including for example, when an assessment is required, how to obtain it, required documentation, timelines, language and format rules, responsible authority and contact details, legal basis, appeal procedures, and interactions with other assessments (e.g. Data Protection Impact Assessments, DPIAs).
    a) While member states are responsible for ensuring that this information exists, HDABs should provide or facilitate access to it before and during the application process.
- Where national law requires an ethics review, the applicant is responsible for obtaining it. The HDAB must ensure that the applicant provides proof that the approval is in place.

8 Article 52(3) – Intellectual property rights and trade secrets

Article 52 in the EHDS regulation establishes a specific framework to protect IPR and trade secrets attached to health data made available under the EHDS regulation.

Although not part of the legal grounds to assess permitted or prohibited purposes under Articles 53 and 54, Article 52(3) is relevant when a lawful purpose cannot be implemented due to unresolved IPR or trade secret concerns. Therefore, this section provides complementary guidance for HDABs.

Under Article 52(3) HDABs shall take all specific appropriate and proportionate measures, including legal, organisational and technical measures, they deem necessary to protect the intellectual property rights, trade secrets or the regulatory data protection right laid down in Article 10(1) of Directive 2001/83/EC[21] or Article 14(11) of Regulation (EC) 726/2004[22]. HDABs shall remain responsible for determining whether such measures are necessary and appropriate.

Directive 2001/83/EC, Article 10(1), governs the re-use of toxicological and clinical trial data in the context of marketing authorisation for generics, with specific protection periods. These provisions serve as reference points for determining the regulatory data protection that HDABs must take into account under Article 52(3).

The second reference, to the Regulation (EC) 726/2004 (dealing with authorisation and supervision of medicinal products for human use), Article 14(11), defines concerns periods of data protection and marketing protection for medicinal products for human use which have been authorised in accordance with that same regulation.

The legislator´s intentions are stated in Recital 60 of the EHDS regulation: Electronic health data protected by intellectual property rights or trade secrets, including data on clinical trials, investigations and studies, can be very useful for secondary use and can foster innovation within the Union for the benefit of Union patients. In order to incentivise continuous Union leadership in this domain, it is important to encourage the sharing of clinical trials and clinical investigations data through the EHDS for secondary use. Clinical trials and clinical investigations data should be made available to the extent possible, while taking all necessary measures to protect intellectual property rights and trade secrets. EHDS regulation should not be used to reduce or circumvent such protection and should be consistent with the relevant transparency provisions laid down in Union law, including for clinical trials and clinical investigations data. Health data access bodies should assess how to preserve such protection while enabling access to such data for health data users to the extent possible. If a health data access body is unable to provide access to such data, it should inform the health data user and explain why it is not possible to provide such access. Legal, organisational and technical measures to protect intellectual property rights or trade secrets could include common electronic health data access contractual arrangements, specific obligations within the data permit in relation to such rights, pre-processing the data to generate derived data that protect a trade secret but nonetheless have a utility for the

[21] Directive 2001/83/EC of the European Parliment and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use: Directive - 2001/83 - EN - EUR-Lex
[22] Regulation (EC) No 726/2004 of the European Parliament and of the Council of 31 March 2004 laying down Community procedures.

health data user or configuration of the secure processing environment so that such data are not accessible to the health data user.

Article 52(3) does not concern the allowed purposes and prohibited secondary use in Articles 53 and 54, but rather the conditions and limitations under which data are made available. However, DG SANTÉ has during the work with task 5.2.1 highlighted that HDABs are responsible for assessing applications and ensuring that data access is lawful, proportionate and secure, why it is important that HDABs are aware of how Article 52(3) may intersect with their role, in particular when:

- Evaluating whether specific data fields should be withheld or anonymised due to trade secrets;
- Ensuring that the data permit explicitly reflects any limitation imposed by the health data holder;
- Responding to health data users' questions about permitted reuse or the handling of sensitive commercial information.

Therefore, Article 52(3) is mentioned in this guideline.

8.1.1 General reflections

Health data holders must notify the HDABs if their dataset contains information covered by IPR or trade secrets, either when submitting the dataset description for inclusion in the dataset catalogue or later when a permit or request for such data are issued (Article 52(2)).

HDABs are then responsible for ensuring that all necessary and adequate safeguards are imposed to preserve the confidentiality of IPR, under Article 52(3). Hence, the assessment also includes taking into account the relevant rights of both the health data holder and health data user (Article 57(1)(c)). If HDABs conclude that there are insufficient safeguards to protect IPR or trade secrets, it may reject the permit application on these grounds (Article 52(5)).

Legal, organisational and technical measures to protect IPR or trade secrets could include common electronic health data access contractual arrangements, specific obligations within the data permit in relation to such rights, pre-processing the data to generate derived data that protect a trade secret but nonetheless have a utility for the health data user or configuration of the secure processing environment so that such data are not accessible to the health data user (Recital 60).

The practical implementation of Article 52(3) by member states remains unclear, with few concrete examples available despite the efforts of task 5.2.1. Workshop discussions did not yield additional examples beyond those already mentioned in Recital 60. To support implementation, further clarification and experience-sharing — particularly through continued exchanges between HDABs and health data holders — may be necessary to develop a library of viable practices.

8.1.2 Recommendations

- HDABs should always specifically consider if the data is limited according to Article 52(3) and the necessity of taking measures to protect IPR and trade secrets, before granting a data permit.
- HDABs should verify that the dataset description includes explicit notice from the health data holder if any data fields are covered by IPR or trade secrets, in accordance with Article 52(2).
    - For further guidance on the assessment, step by step, see Guideline for HDABs on the procedures and formats for data access (T6.3)
- HDAB should investigate the meaning of legal, organisational or technical protection measures in order to find applicable practical examples, as well as what are considered sufficient protective measures in terms of IPR and trade secrets. Perhaps this will be explained in written contributions issued by the EHDS Board that is to be set out (see Recital 95).
- Develop a best practice list, which over time can serve as support for HDABs, including ensuring that assessments within member states become uniform. Otherwise, there is a risk that different member states make different assessments based on the same conditions. A suggested solution is to place the responsibility for this list with the EHDS Board.
- Develop a checklist that includes a summary of actions HDABs have to take when handling IPR and trade secrets.

9 Areas of further exploration?

The following sections includes questions and matters that still need further refinement in order to be used in practice as a recommendation. For instance, it includes processes, procedures and systems in need of clarification. The content of this section has not been an issue for the major contributor team but needs further insights and analysis if it is to be included in the deliverable.

9.1 Continuous alignment between HDABs on the assessment

The work of this task regarding Articles 53, 54 and 52(3) should not end with the finalisation of this deliverable. A review needs to be done by the organisation responsible for revising the relevant information in the guideline, after the experiences received during the work with allowed purposes and prohibited secondary use. The question is by whom this review should be done, e.g. the central HDAB, a cooperation between coordinating HDABs in each country, or a possible secondary use subgroup of the EHDS Board, and how it should be done. It is crucial that the information is updated and revised yearly to maintain its validity also in the future. Thus, it is a governance gap to be fixed.

9.2 Clarifying the boundaries between innovation and marketing

While Article 54(c) under the EHDS regulation clearly prohibits the use of electronic health data for marketing or advertising purposes, it is essential to help HDABs distinguish between legitimate innovation (permitted under Article 53(e)) and marketing misuse. Without clear boundaries and definitions, HDABs risk either stifling innovation by treating all commercial actors with suspicion or allowing overly broad interpretations that lead to misuse, both of which can erode public trust and increase opt-outs, ultimately harming innovation and public health.

A key criterion is whether the data obtained under the EHDS framework is used to support product development (permitted) or to target specific audiences or influence behaviour for commercial promotion (prohibited). For example, a health data user may develop a new medical device or AI tool using health data obtained via a permit but is allowed not to use that data to identify facilities or patients or even regions with increased marketing potential for marketing purposes once the product is completed.

To support consistent interpretation and enforcement, HDABs should be equipped with practical guidance, including examples, indicators, and red flags, that help identify when a proposed use may drift into prohibited territory under Article 54(c). Vague or overly generic objectives such as “market analysis,” “user testing,” or “consumer insights” should be flagged for further scrutiny, as they may conceal marketing intentions. Monitoring and post-permit traceability tools may also help safeguard against misuse.

Any data use beyond the scope of the issued permit, including for marketing purposes, is prohibited and subject to sanctions under Articles 63 and 64.

9.3 Interpretation of Article 54(d) in relation to medical research involving controlled substances

Article 54(d) of the EHDS regulation prohibits the secondary use of health data for developing illicit drugs, but it does not clearly define what constitutes an “illicit drug,” nor does it explicitly address whether medical research involving them or controlled substances is permissible. While legislation such as Directive (EU) 2017/2103 provides certain definitions, these are non-exhaustive and may vary across member states.

The classification of narcotics evolves continuously and includes a wide range of central nervous system-active compounds. Many of these substances are used in regulated medical contexts or are being actively studied for therapeutic purposes. Some were not originally developed as narcotics but have since been misused.

This raises important questions: Should HDABs automatically reject applications involving such substances, even if the declared purpose is legitimate medical research, such as developing improved treatments for ADHD or depression? What if the substance is legal in some member states but prohibited in others? Without clearer guidance, HDABs may struggle to distinguish between prohibited misuse and permissible scientific research.

It is essential to emphasize that under no circumstances should the EHDS framework be interpreted in a way that promotes or normalizes the use of narcotics. Substance abuse is a serious societal issue and a major contributor to individual and public health problems. However, in the context of responsible, ethically approved medical research, it may be necessary to explore all scientifically valid options to develop effective treatments for conditions such as severe depression or neurological disorders. This requires an extremely careful balance between public health protection and enabling innovation.

9.4 Standard European procedure regarding the HDAB’s assessment

Voluntary convergence on application assessment procedures across member states may begin through collaborative forums such as the HDABs Community of Practice, which is already mandated to promote best practices. Standard European procedures and corresponding guidelines for HDABs are not formally established at this stage, but practical alignment can be encouraged by developing shared examples, reference tools or informal ”gold standards”. The HDABs Community of Practice could serve as a starting point and valuable mechanism for this. The outcomes of the Community of Practice should be documented in written form, ideally as a guideline that is reviewed and updated annually by, for example, a potential secondary use subgroup of the EHDS Board, given that the Community of Practice is only a temporary structure. If such a subgroup is not established, or lacks the necessary resources or mandate, an alternative mechanism for regular review and adjustment will need to be put in place. As this review mechanism is not explicitly foreseen in the regulation, it constitutes a governance gap that should be addressed.

However, it should be acknowledged that no best practice can fully capture all scenarios, particularly given that each use case may raise unique risks of prohibited secondary uses. Therefore, extreme clarity must be applied when articulating assessment expectations, procedures, and responsibilities.

9.5 Arrangement of ethical and legal support in the HDABs assessment process

HDABs are expected, under the EHDS regulation, to possess or have access to sufficient legal and technical expertise in-house to carry out their assessment tasks in accordance with Articles 53, 54 and 52(3) (see Article 55(2)). This includes the ability to identify when a request may trigger concerns regarding prohibited secondary use.

However, national law may impose ethical assessment obligations in specific cases. In line with Article 67(2)(j) and Recital 73, member states retain full competence over ethics provisions and are responsible for organising appropriate support mechanisms. These may include:

- ensuring HDABs have access to national ethics bodies, or
- embedding ethical expertise within the HDAB, with clear links to existing ethics review structures.

That said, not all aspects of Article 54 involve ethical considerations — some prohibited uses relate to discrimination, marketing or harmful products. Therefore, it should not be implied that ethics review alone can safeguard against all breaches of Article 54. Instead, HDABs must ensure that their legal assessment procedures are robust and clearly documented, and that roles and responsibilities are properly delineated.

In the longer term, it may merit discussion whether a centralised EU-wide ethics body would be beneficial. Such a body could be composed of ethics experts from each member state and serve several important functions. It could act as an information hub, providing clear guidance to applicants on how ethical assessment is conducted in each country, what documentation is required, and how to comply with national procedures. Additionally, it could advise on country-specific ethical requirements, helping ensure that national rules are respected while streamlining the experience for applicants navigating a fragmented legal and ethical landscape. Over time, the body could also evolve to take on a more operational role, carrying out ethical assessments itself. With representation from national experts, it would be well-positioned to offer country-specific evaluations, ultimately serving as a centralised, ‘single application’ solution for ethical review across the EU.

However, while the idea of such an EU-level support service may merit discussion in the future, it goes beyond the current scope of the EHDS regulation and this deliverable. Thus, instead of a recommendation this is a suggestion for future policy discussions.

For now, clarity is needed on how each member state ensures that HDABs are equipped to deal with legal and ethical complexity in line with national frameworks. Given the current possibilities, a viable solution would be to map national ethical requirements and make them publicly accessible via the EHDS Board or HealthData@EU. This could support the transparency for data users and HDABs.

Beyond simply involving health data holders or trusted health data holders, there is also a need to develop structured processes that facilitate the continuous flow of knowledge between health data holders, HDABs, and health data users. Such processes could enable not only better understanding of data composition and suitability but also support active data

stewardship, promote transparency, and drive improvements in data quality. By fostering two-way feedback loops — from health data holders to users and back again — these mechanisms can contribute to more accurate applications, more informed assessments, and ultimately, higher-quality data ecosystems.

9.6 Automated decision-making and other decisions detrimental to individuals or groups

From Article 54(a) and Recital 62 can be read that automate decision-making could be harmful to individuals and therefore prohibited under the EHDS regulation. Not only does this require HDABs to have relevant competence to make a correct assessment of such systems and uses; it also raises questions on how far an HDAB must go in its investigations in order to be able to assess a potential prohibited use.

Further, in situations involving AI and automated decision-making, it is not clear from the EHDS regulation if HDABs are to demand transparency and other possible characteristics – depending on the nature of the AI system, innovation et cetera – from the health data user (Article 54 (a–b)). However, it is clear that for AI systems suspected of being used in violation of Article 5 of the AI Act (Prohibited AI practices), HDABs should require satisfactory information to ensure that the data made available is not used to develop prohibited systems and practices. Therefore, in relevant situations, complementary checks ought to be made in the review process under Article 54(a). Perhaps the EHDS Board can develop minimum transparency indicators or checklists for HDABs to apply in such cases.

9.7 Building a monitoring system for identifying possible misuse

Nationally this could be a separate part or a department of an HDAB that conducts random or systematic audits to ensure health data users have used health data only as permitted and not for prohibited purposes. In the case of multiple HDABs, this responsibility could be allocated, based on Article 55(1) of the EHDS regulation to a single HDAB, not necessarily to the coordinator one, to avoid duplication of resources and to enhance the quality and consistency of the assessment.

Instead of assigning numerical scores, a **voluntary, qualitative risk rating** could be introduced based on monitoring outcomes, allowing HDABs to better assess potential risks while respecting transparency, proportionality, and data protection rights. Other HDABs could refer to an existing qualitative risk rating when evaluating the likelihood of prohibited data use under Article 54.

It should be considered that it is difficult for the HDABs to find misuse, and usually only significant violations can be identified. Furthermore, the EHDS regulation does not specify how long HDABs should have a monitoring function. The necessary monitoring timeframe may depend on the type of health data user (e.g., a cigarette company that might use the information to make its products less carcinogenic but still addictive, versus a university hospital posing lower risks), the nature of the health data, and the claimed usage.

Finally, the possibility of establishing a European-level follow-up mechanism is flagged as a suggestion for future policy discussions beyond the scope of the current EHDS Regulation.

This could be considered either instead of, or in addition to the described national mechanism.

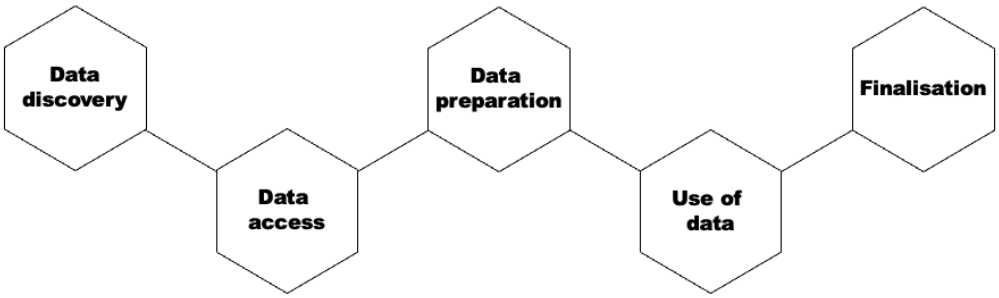
Annex index

Annex number	Annex title
1	User journey
2	Methodology
3	Links to relevant EHDS articles and recitals
4	Glossary
5	Figure 1 enlarged

Annex 1 User Journey

When a data user[23] applies for electronic health data for secondary use purposes, such as research and innovation activities, education, and policy-making, within the European Health Data Space (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)[24]. 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)[25] deliver(s) the necessary data to the HDAB, which starts to prepare the data for secondary use. Techniques for pseudonymisation,

[23] Data user = a person using electronic health data for a secondary use purpose

[24] Health data access body (HDAB) = the authority responsible for assessing the information provided by the data user who applies for electronic health data for a secondary use purpose

[25] Data holder = Any natural or legal person, public authority or other body in the healthcare or the care sectors that has the right or obligation to provide electronic health data for secondary use purposes or the ability to make such data available (see more EHDS Regulation Art. 2 (1t)).

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.[26] 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.

[26]Secure processing environment = an environment with strong technical and security safeguards in which the data user can process personal level electronic health data

Annex 2 Methodology

The guideline is based on working group discussions (online meetings), individual desk research, expert interviews and results from discussions in three separate workshops with open participation from relevant stakeholders.

Workshops and discussion

The workshop series was led by the major contributors in task 5.2.1, namely the Swedish e-health Agency (SEHA), the Swedish National Board of Health and Welfare (NBHW), the Danish Health Data Authority (DHDA), the Finnish Institute for Health and Welfare (THL), the Austrian National Public Health Institute (GÖG) and the Technology and Methods Platform for Networked Medical Research e.V. (TMF).

The TEHDAS2 community along with other stakeholders and external experts were invited for discussion. Professional representatives have included legal and technical expertise concerning health data infrastructure and health data policy from member states as well as non-member states. These include future key stakeholders such as health data holders, HDABs and health data users. In addition, international organisations such as the World Health Organisation (WHO), the European Commission, Eurostat, the Commission's Health and Digital Executive Agency and the OECD also participated. The countries that were represented in the workshops included Sweden, Austria, Denmark, Finland, Belgium, Spain, Croatia, Greece, Germany, The Netherlands, Italy, Iceland, Hungary, Ireland, France, Luxembourg, Ukraine, Latvia, Lithuania, Malta, Norway, Czech Republic and Slovenia. There were between 80 and 120 participants in each workshop.

The aim of the workshop series was to clarify, through discussion and shared experiences, the purposes for which health data can and cannot be used, as according to Articles 53, 54 and 52(3). The workshops focused on the role of HDABs in enabling the secondary use of electronic health data under EHDS. Discussions aimed at

- clarifying concepts and definitions,
- interpretation of allowed purposes and prohibited data use and
- exploring possible consequences for the assessment process of HDABs.

Each workshop was organised according to specific topics under Articles 53, 54 and 52(3) as summarised in the following table.

Table 4. Workshops

Topic	Articles
Workshop 1 Prohibited secondary use	Article 54, Article 52(3)
Workshop 2 Purposes	Article 53 e–f e) Scientific research f) Provision of care

Workshop 3 Purposes	Article 53 a–d a) Public interest b) Policymaking c) Statistics d) Education

The information received in the workshops has been analysed and incorporated in the guideline.

Expert interviews

In addition, three expert interviews have been held with representatives from Vall d'Hebron Research Institute, Statistics Sweden and Finnish Social and Health Data Permit Authority (Findata) in order to acquire in-depth knowledge on certain topics.

Drafting and review process

The first draft of the Milestone has been developed by the major contributors of task 5.2.1 between April and June 2025. Each major contributor has been responsible for a section of the final report. In a weekly meeting upcoming questions and changes have been discussed. Collaborative tools and methodologies were used to draft the specification. This allowed for real-time input and revisions from all participants, ensuring a transparent and inclusive writing process. Desktop analysis of existing information has been performed.

Parts of the Milestone has been reviewed by the Review board of the work package, consisting of representatives from five countries, as well as the European Commission Directorate-General for Health and Food Safety (DG SANTÉ). DG SANTÉ has also provided input by giving guidance on questions concerning the interpretation of the regulation. The Milestone has furthermore been reviewed by Sitra, the members of the Project Steering Group of TEHDAS2 and DG SANTÉ before the public consultation. This Milestone will then in addition be reviewed through public consultation.

Annex 3 Links to relevant EHDS articles and recitals

Articles 53, 54 and 52(3) of the EHDS regulation[27], as well as the relevant recitals, are summarised in Table 3 and presented in full version below.

Table 5 Summary of EHDS articles and relevant recitals.

Articles	Recitals
Article 53	Recital 61
Article 54	Recital 62
Article 52(3)	Recital 60

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

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

   (a) the public interest in the areas of public or occupational health, such as activities to protect against serious cross-border threats to health, public health surveillance or activities ensuring high levels of quality and safety of healthcare, including patient safety, and of medicinal products or medical devices;

   (b) policy-making and regulatory activities to support public sector bodies or Union institutions, bodies, offices or agencies, including regulatory authorities, in the health or care sector to carry out their tasks defined in their mandates;

   (c) statistics as defined in Article 3(1) of Regulation (EU) No 223/2009, such as national, multi-national and Union-level official statistics, related to health or care sectors;

   (d) education or teaching activities in health or care sectors at vocational or higher education level;

   (e) scientific research related to health or care sectors that contributes to public health or health technology assessments, or ensures high levels of quality and safety of healthcare, of medicinal products or of medical devices, with the aim of benefiting end-users, such as patients, health professionals and health administrators, including:

      (i) development and innovation activities for products or services;

      (ii) training, testing and evaluation of algorithms, including in medical devices,

      (iii) in vitro diagnostic medical devices, AI systems and digital health applications;

[27] Regulation (EU) 2025/327 on EHDS, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL_202500327.

(f) improvement of the delivery of care, of the optimisation of treatment and of the provision of healthcare, based on the electronic health data of other natural persons.

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

Article 54 Prohibited secondary use

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

In particular, seeking access to and processing electronic health data obtained via a data permit issued pursuant to Article 68 or a health data request approved pursuant to Article 69 for the following uses shall be prohibited:

(a) taking decisions detrimental to a natural person or a group of natural persons based on their electronic health data; in order to qualify as 'decisions' for the purposes of this point, they have to produce legal, social or economic effects or similarly significantly affect those natural persons;

(b) taking decisions in relation to a natural person or a group of natural persons in relation to job offers, offering less favourable terms in the provision of goods or services, including exclusion of such persons or groups from the benefit of an insurance or credit contract, the modification of their contributions and insurance premiums or conditions of loans, or taking any other decisions in relation to a natural person or a group of natural persons which result in discriminating against them on the basis of the health data obtained;

(c) carrying out advertising or marketing activities;

(d) developing products or services that may harm individuals, public health or society at large, such as illicit drugs, alcoholic beverages, tobacco and nicotine products, weaponry or products or services which are designed or modified in such a way that they create addiction, contravene public order or cause a risk for human health;

(e) carrying out activities in conflict with ethical provisions laid down in national law.

Article 52(3) Intellectual property rights and trade secrets

3. Health data access bodies shall take all specific appropriate and proportionate measures, including of a legal, organisational and technical nature, they deem necessary to protect the intellectual property rights, trade secrets or the regulatory data protection right laid down in Article 10(1) of Directive 2001/83/EC or Article 14(11) of Regulation (EC) 726/2004. Health data access bodies shall remain responsible for determining whether such measures are necessary and appropriate.

Recital 61

The secondary use of health data under the EHDS should enable public, private and not-for-profit entities, as well as individual researchers, to have access to health data for research, innovation, policymaking, educational activities, patient safety, regulatory activities or personalised medicine, in line with the purposes as set out in this Regulation. Access to data for secondary use should contribute to the general interest of society. In particular, the secondary use of health data for research and development purposes should contribute to benefiting society in the form of new medicines, medical devices, and healthcare products and services at affordable and fair prices for Union citizens, as well as to enhancing access to and the availability of such products and services in all member states. Activities for which access in the context of this Regulation is lawful could include using the electronic health data for tasks carried out by public sector bodies, such as the exercise of public duty, including public health surveillance, planning and reporting duties, health policymaking, and ensuring patient safety, quality of care and the sustainability of healthcare systems. Public sector bodies and Union institutions, bodies, offices and agencies might need to have regular access to electronic health data for an extended period of time, including in order to fulfil their mandate, as is provided for in this Regulation. Public sector bodies could carry out such research activities by using third parties, including sub-contractors, as long as the public sector body remains at all times the supervisor of those activities. The provision of the data should also support activities related to scientific research. The notion of scientific research purposes should be interpreted in a broad manner, including technological development and demonstration, fundamental research, applied research and privately funded research. Activities related to scientific research include innovation activities such as training of AI algorithms that could be used in healthcare or the care of natural persons, as well as the evaluation and further development of existing algorithms and products for such purposes. It is necessary that the EHDS also contribute to fundamental research, and, although its benefits to end-users and patients might be less direct, such fundamental research is crucial for societal benefits in the longer term. In some cases, the information of some natural persons, such as genomic information of natural persons with a certain disease, could contribute to the diagnosis or treatment of other natural persons. There is a need for public sector bodies to go beyond the scope of 'exceptional need' of Chapter V of Regulation (EU) 2023/2854. However, health data access bodies should be allowed to provide support to public sector bodies when processing or linking data. This Regulation provides for a channel for public sector bodies to obtain access to information that they require for fulfilling the tasks assigned to them by law, but does not extend the mandate of such public sector bodies.

Recital 62

Any attempt to use electronic health data for measures detrimental to natural persons, such as to increase insurance premiums, to engage in activities potentially detrimental to natural persons related to employment, pensions or banking, including mortgaging of properties, to advertise products or treatments, to automate individual decision-making, to re-identify natural persons or to develop harmful products should be prohibited. That prohibition should also apply to activities contrary to ethical provisions under national law, with the exception of ethical provisions relating to consent to the processing of personal data and ethical provisions relating to the right to opt out, since this Regulation takes precedence over national law in accordance with the general principle of the primacy of Union law. It should also be prohibited

to provide access to, or otherwise make available, electronic health data to third parties not mentioned in the data permit. The identity of authorised persons, in particular the identity of the principal investigator, who will have the right pursuant to this Regulation to access electronic health data in the secure processing environment should be indicated in the data permit. The principal investigators are the main persons responsible for requesting access to the electronic health data and for processing the requested data within the secure processing environment on behalf of the health data user.

Recital 60

Electronic health data protected by intellectual property rights or trade secrets, including data on clinical trials, investigations and studies, can be very useful for secondary use and can foster innovation within the Union for the benefit of Union patients. In order to incentivise continuous Union leadership in this domain, it is important to encourage the sharing of clinical trials and clinical investigations data through the EHDS for secondary use. Clinical trials and clinical investigations data should be made available to the extent possible, while taking all necessary measures to protect intellectual property rights and trade secrets. This Regulation should not be used to reduce or circumvent such protection and should be consistent with the relevant transparency provisions laid down in Union law, including for clinical trials and clinical investigations data. Health data access bodies should assess how to preserve such protection while enabling access to such data for health data users to the extent possible. If a health data access body is unable to provide access to such data, it should inform the health data user and explain why it is not possible to provide such access. Legal, organisational and technical measures to protect intellectual property rights or trade secrets could include common electronic health data access contractual arrangements, specific obligations within the data permit in relation to such rights, pre-processing the data to generate derived data that protect a trade secret but nonetheless have a utility for the health data user or configuration of the secure processing environment so that such data are not accessible to the health data user.

Annex 4 Glossary

This is a living document to be updated throughout the joint action.

The latest updates: 05/09/2025

The major terms used in Milestone 5.2 is highlighted in grey.

Term	Definition
Access permit	Machine-actionable data structure that contains the information from data permit in a standardised format that can be securely transferred and acted on by computer services
Access point	A component of the HealthData@EU infrastructure that ensures secure, point-to-point message exchange between National Contact Points and the central platform. Access Points exist at both the national and EU levels and enable the technical interconnection required by Articles 36(3d) and 75 of the Regulation.
Additional information (related to pseudonymisation)	Additional information is information whose use enables the attribution of **pseudonymised data** to identified or identifiable persons (EDPB Guideline 01/2025 Glossary, version adopted for public consultation). This term is specific to **pseudonymisation** and related to the "additional information" referred to in Regulation (EU) 2016/679 Article 4(5) (GDPR).
AI systems	'AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. (AI Act – Regulation (EU) 2024/1689, Article 3(1))
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

Term	Definition
	2019 on open data and the re-use of public sector information, Recital 52; EHDS Regulation, Recital 92)
Anonymisation metadata	Anonymisation metadata refers to a structured set of detailed information describing (a) the methods and parameters used to anonymise a dataset, and (b) the resulting **quality metrics** used to anonymise a dataset or data processing result, or to assess their anonymisation. It includes details e.g., on applied techniques and transformation logs. This metadata helps assess data protection, track modifications, and ensure compliance with anonymisation criteria.
Anonymisation result	The output of anonymisation, which can be an anonymised dataset or a data processing result including **anonymisation metadata**.
Anonymised statistical format	An anonymised statistical format refers to aggregated data that does not include information on individual data subjects or entities, also labelled as non-personal aggregated data.
Areas of Occupational Health	'Public health' shall mean all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality (Regulation (EU) 1338/2008, Annex V, (b) and WHO2, Article 3(c))
Areas of Public Health	'Public health' shall mean all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality (Regulation (EU) 1338/2008)
Attribution of pseudonymised data to data subjects	Process that establishes that **pseudonymised data** relate to an already identified person, or links the data to other information with reference to which the data

Term	Definition
	subjects could be identified. (EDPB Guideline 01/2025 Glossary, version adopted for public consultation)
Authorised user	An authorised natural person listed in the data permit, giving them the rights to process sensitive data inside an SPE
Benefits (of data use)	Refers broadly to positive outcomes of data use. It can encompass social, health and environmental aspects, among others.
Central Platform	An interoperability platform established by the European Commission, providing services to support and facilitate the exchange of information between National Contact Points and authorised participants in HealthData@EU for secondary use of electronic health data. (EHDS Regulation, Article 75(8))
Consistent pseudonymisation	Two sets of data are considered to be pseudonymised consistently if data contained in those sets and relating to the same person can be linked on the basis of the **pseudonyms** they contain (EDPB Guideline 01/2025 Glossary, version adopted for public consultation). Consistency is context-specific and may be limited to a **pseudonymisation domain**.
Cross-border gateway	Handles the transmission and reception of communications between one National Contact Point and Central Services in a secure and technically standardised manner. It supports the eDelivery protocol (HD@EU Pilot WP5 – Architecture Definition).
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 aggregation	A process by which information is collected, manipulated and expressed in summary form (ISO/TR 12300:2014(en), 2.1.4)

Term	Definition
Data anonymisation framework	A set of processes and practices designed to ensure data privacy through anonymisation and **privacy risk assessment**.
Data combination	The process of bringing together data from multiple ***datasets*** that can be processed pursuant to one or multiple data permit(s) or data request(s) (Regulation (EU) 2015/327 (EHDS) Articles 57, 68, 69) or other legal basis (such as consent or permits based on other legislation than EHDS). ***Data linkage*** can be part of this process.
Data consolidation	A process of combining data from multiple sources, cleaning and verifying them, removing errors so that they can be prepared for provision. Data consolidation may include creation of data subsets, data extraction, duplicates elimination, quality control and data linkage aspects.
Data controller	A data controller is a person or organisation that determines the purposes and essential means of the processing of personal data. The role of the data controller can be shared by several people or organisations. In that case, they are defined as joint controllers. The controller is accountable and responsible for establishing a lawful data processing workflow and observing the rights of data subjects. (GDPR Article 4(1)(7)).
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.

Term	Definition
Data holder application (a software linked to the Secure Processing Environment)	A software application that provides the data holder with secure digital access to the Secure Processing Environment (SPE). Its core functions include facilitating the upload and download of data in accordance with the data holder's responsibilities under the EHDS Regulation.
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 preparation	Data preparation is the process in which an organisation (in this case the data holder) transforms and organises raw personal or non-personal health data into one or more datasets (either in individual-based or aggregated form), to comply with a data permit or a data request approval issued by a data user and approved by the competent Health Data Access Body.

Term	Definition
Data processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. (GDPR Article 4(2))
Data processing result	Data processing result refers to outputs from data processing activities carried out by the health data user. It may be generated from statistical analysis or machine learning algorithms, including descriptive statistics, model coefficients, performance indicators, visualisations.
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))
Data protection	The "implementation of appropriate administrative, technical or physical means to guard against unauthorized intentional or accidental disclosure, modification, or destruction of data (ISO/IEC 20944-1:2013(en), 3.6.5.1).
Data provenance	Data provenance means a **description of the source** of the data, including context, purpose, method and technology of data generation, documenting agents involved in the provenance of data, data validation routines, source data verification, traceability of changes, and quality control of data.
Data provision	The stage in the data user journey where prepared health data is made accessible to authorised users for secondary purposes.
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(2z))
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(2aa))

Term	Definition
Data user application (a software linked to the Secure Processing Environment)	A software application that provides the data user with secure, computerised access to their workspace within the Secure Processing Environment. Its primary functions include facilitating the upload and download of data while ensuring robust authentication and authorisation mechanisms to prevent unauthorised access.
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(2y))
Dataset record	A dataset record is a single, structured unit of data within a dataset, analogous to a row in a table or a record in a database. It contains specific information about a single entity or instance within the broader dataset.
Dataset subset	Dataset subset contains only selected records, variables or elements 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))
Direct identifier	A data element (or set thereof) that has been assigned or is being used to distinguish the data subject it refers to from all others in the given context without requiring the use of **additional information**. Examples are passport or social security number, or the set consisting of first and last name as well as date of birth. (EDPB Guideline 01/2025 Glossary, version adopted for public consultation)
Disclosure control	Disclosure control refers to techniques and procedures applied to datasets to reduce the privacy risks for individuals when the data is disclosed to data users.
Dispatcher	A component of the HealthData@EU infrastructure that enables the secure transmission, routing and delivery of structured electronic messages (such as dataset

Term	Definition
	records and access requests) between national and central systems.
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))
Federated analysis	A decentralised approach to data analysis where statistical results are computed locally on distributed data resources rather than aggregating raw data centrally. This method enables benchmarking, multi-site research, and collaborative analytics while preserving data privacy and security. Only aggregated insights or summary statistics are shared between nodes, ensuring compliance with data protection regulations.
Federated learning	A decentralised machine learning approach where models are trained and validated on distributed data resources without transferring raw data. Instead, only model updates or gradients are exchanged between nodes, enhancing data privacy and security. This method enables collaborative model development across multiple organisations or devices while maintaining local data sovereignty and regulatory compliance.
Federated processing	A decentralised data processing approach where computations occur locally on distributed nodes rather than being centralised. This method enables data to remain on local devices or servers while only aggregated results or model updates are shared, enhancing privacy and security. It is commonly used in

Term	Definition
	machine learning (“federated learning”), analytics (“federated analysis”), and secure data collaborations across multiple organisations.
Fidelity	Fidelity (or resemblance**)** refers to the extent to which processed data—such as anonymised data—retains the statistical properties, relationships, and structural characteristics of the **original data**. High fidelity means that distributions, correlations, and key patterns remain intact.
Healthcare	‘Healthcare’ means health services provided by health professionals to patients to assess, maintain or restore their state of health, including the prescription, dispensation and provision of medicinal products and medical devices. (Directive 2011/24/EU, Article 3(a))
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 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 Regulation.
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

Term	Definition
	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(2t))
Health data request	A request to access data in an anonymised statistical format for the purposes referred to in EHDS Article 53. (EHDS Regulation, 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 Regulation, Article 2(2u))
Health technology assessment	'Health technology assessment' or 'HTA' means a multidisciplinary process that summarises information about the medical, patient and social aspects and the economic and ethical issues related to the use of a health technology in a systematic, transparent, unbiased and robust manner; (Regulation (EU) 2021/2282, Article 2(5))
High Performance Computing (HPC)	HPC is the use of advanced and not commonly available computational infrastructure – such as supercomputers or compute clusters – to solve highly complex and resource intensive computational problems.
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) No 1610/96 of the

Term	Definition
	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. (Regulation concerning customs enforcement of intellectual property rights and repealing, Article 2(1))
Intermediation entity	A legal person that may be established by national law for the purpose of fulfilling the obligations of certain categories of health data holders and that is able to process, make available, register, provide, restrict access to and exchange electronic health data for secondary use provided by health data holders. (EHDS Regulation, Article 50 (3) and Recital 59)
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 Regulation, Article 2(2f))
Irreversible pseudonymisation	A pseudonymisation method where the **pseudonymising transformation** cannot be reversed. The information necessary to re-establish the link between the **pseudonym** and the **original data** has been permanently destroyed or is otherwise unavailable.
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

Term	Definition
	secondary use are laid down in EHDS Regulation, Article 53.
Medicinal product	'Medicinal' product means any substance or combination of substances presented for treating or preventing disease in human beings. Any substance or combination of substances which may be administered to human beings with a view to making a medical diagnosis or to restoring, correcting or modifying physiological functions in human beings is likewise considered a medicinal product. (Directive 2011/24/EU referring to Directive 2001/83/EC, Article 1(2))
Medical device	'Medical device' means any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes: - diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease, - diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability, - investigation, replacement or modification of the anatomy or of a physiological or pathological process or state, - providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations, and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means. The following products shall also be deemed to be medical devices: - devices for the control or support of conception; - products specifically intended for the cleaning, disinfection or sterilisation of devices as

Term	Definition
	referred to in Article 1(4) and of those referred to in the first paragraph of this point. (Regulation (EU) 2017/745 and (EU) 2017/746, Article 2(1))
Metadata	A structured description of the contents or the use of data facilitating the discovery or use of that data. (Data Act, Article 2)
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-compliance	Any failure to comply with any requirement under the Union harmonisation legislation.
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. (EHDS Regulation, Article 2(2b))
Observational Medical Outcomes Partnership (OMOP) common data model (CDM)	A standardised, common data model (CDM) specification originally developed by the Observational Medical Outcomes Partnership (OMOP) and now maintained by the Observational Health Data Sciences and Informatics (OHDSI) community. It defines a consistent structure and a set of standardised vocabularies for observational health data, enabling researchers to perform large-scale, reproducible analyses across diverse databases.
Open data	Data in an open format that can be freely used, re-used and shared by anyone for any purpose. Open format means a file format that is platform-independent and made available to the public without

Term	Definition
	any restriction that impedes the re-use of documents. (EU Open Data Directive)
Open (data) database	Publicly accessible digital data that anyone can freely use, reuse, and redistribute for any purpose.
Original data	Individual-level health data prior to any application of **pseudonymisation, anonymisation**, or **synthetic data generation**. It consists of raw data that directly represent real-world individuals.
Personal electronic health data	Data concerning health and genetic data, relating to an identified or identifiable natural person, processed in an electronic form. (EHDS Regulation, Article 2(2a))
Privacy (of synthetic or anonymised data)	Privacy measures the extent to which anonymised or synthetic data protects individuals from re-identification, membership inference, or sensitive information leakage. High privacy ensures that no single individual can be traced back to the real dataset, nor can their participation in the **dataset** be inferred.
Privacy risk assessment	Overall process of identifying, analysing, evaluating, consulting, communicating and planning the treatment of potential privacy impacts with regard to the processing of personally identifiable information (3.7), framed within an organisation's broader risk management framework (ISO/IEC 29100:2024(en), 3.18). **Re-identification risk assessment** falls under privacy risk assessment, together with attribute inference and group membership, for example.
Pseudonym	Identifier that is added to data during the **pseudonymising transformation** and set in such a way that it can be attributed to data subjects only using **additional information**. (EDPB Guideline 01/2025 Glossary, version adopted for public consultation)
Pseudonymisation	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

Term	Definition
	organisational measures to ensure non-attribution to an identified or identifiable person. (GDPR, Article 4(5))
Pseudonymisation domain	Environment in which the controller or processor wishes to preclude attribution of data to specific data subjects. May incorporate persons acting under the authority of the controller or processor, respectively, other natural or legal persons, public authorities, agencies or other bodies, and their respective technological and informational resources. Does not include persons authorised to process additional data allowing the attribution of the **pseudonymised data** to data subjects. (EDPB Guideline 01/2025 Glossary, version adopted for public consultation)
Pseudonymisation entity	The entity responsible of processing identifiers into pseudonyms using the pseudonymisation function. It can be a data controller, a data processor (performing pseudonymisation on behalf of a controller), a **trusted third party** or a data subject, depending on the pseudonymisation scenario. It should be stressed that, following this definition, the role of the pseudonymisation entity is strictly relevant to the practical implementation of pseudonymisation under a specific scenario. (ENISA, Pseudonymisation techniques and best practices, p. 10)
Pseudonymisation secrets	Data that is used in the application of the **pseudonymising transformation** or is created during that process, for example cryptographic keys or salts, and allows the computation of pseudonyms from certain identifying attributes. Part of **additional information**. (EDPB Guideline 01/2025 Glossary, version adopted for public consultation)
Pseudonymised data	Result of applying the **pseudonymising transformation** to some personal data. Cannot be attributed to a specific data subject without **additional information**. (EDPB Guideline 01/2025 Glossary, version adopted for public consultation)

Term	Definition
Pseudonymising controller or processor	Controller or processor that uses pseudonymisation as a safeguard and modifies **original data** according to Regulation (EU) 2016/679 (GDPR) Article 4(5). (EDPB Guideline 01/2025 Glossary, version adopted for public consultation)
Pseudonymising transformation	Procedure that modifies **original data** in a way that the result cannot be attributed to a specific data subject without **additional information**. (EDPB Guideline 01/2025 Glossary, version adopted for public consultation)
Public sector body	'Public sector body' means the state, regional or local authorities, bodies governed by public law, or associations formed by one or several such authorities or one or several such bodies governed by public law." (Regulation (EU) 2022/868, Data Governance Act, Article 2(17))
Public use file	A **dataset** made available to the public, typically containing anonymised, synthetic or aggregated data to protect individual privacy. These files can be released to data users for information and testing purposes before they apply for a data permit. It is based on **original data**.
Public value (of data use)	Public value means a weighted composite of risks and benefits of the data use taking into account the sustainability of benefits, addressing future societal needs, distributing benefits fairly, evaluating potential harm, ensuring stable safeguards through risk assessment, and correcting any harms that may occur.
Purpose limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. (GDPR, Article 5(1b).
Quality metrics	Quality metrics refer to qualitative and quantitative indicators used to assess the fitness for purpose of a dataset. In the context of synthetic and anonymised data, quality metrics are particularly relevant to evaluate how transformations affect the data's **utility**,

Term	Definition
	fidelity, and **privacy**. Quality metrics may also be used to assess pseudonymised or original datasets, particularly when serving as a benchmark or when evaluating fitness for specific secondary use purposes. (Adapted from ISO and EHDS principles; EHDS Regulation, Article 66 and Recital 58)
Quality metrics evaluation	Quality metrics evaluation refers to the calculation or derivation of the **quality metrics**.
Quality metrics tool	Quality metrics tool (or "metrics tool") refers to a software, an algorithm, a processing pipeline, a documented manual process, or a combination of these, designed to perform **quality metrics evaluation**.
Quasi-identifier	A **dataset** attribute that, when considered in conjunction with other attributes are sufficient to attribute at least part of the pseudonymised data to data subjects. (EDPB Guideline 01/2025 Glossary, version adopted for public consultation)
Re-identification	The process of associating data in a de-identified **dataset** with the original data principal (i.e., data subject) (ISO/IEC 20889:2018(en), 3.31).
Re-identification risk	The risk of a successful re-identification attack (ISO/IEC 20889:2018(en), 3.33), which describes an action performed on de-identified data by an attacker with the purpose of **re-identification** (ISO/IEC 20889:2018(en), 3.32).
Representational State Transfer Application Programming Interface (RESTful API)	An application programming interface used for building scalable and interoperable web services. RESTful API follows the principles of Representational State Transfer (REST), using standard HTTP methods to perform operations on resources identified by URLs. It emphasises stateless interactions, meaning each request contains all necessary information without relying on server-side sessions.
Reversible pseudonymisation	The **pseudonymisation entity** uses a **pseudonymising transformation** process that allows the pseudonymisation entity to reverse the **pseudonym**, if necessary. For example, by using separately kept matching tables of pseudonyms and

Term	Definition
	identifying data, or computable secrets allowing for calculating back to the original input.
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 Regulation, 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 Regulation, Article 73)
Sensitive data	Data with potentially harmful effects in the event of disclosure (i.e., providing access to data to a third party) or misuse (ISO 5127:2017(en), 3.1.10.16)).
Serious cross-border threats	This Regulation shall apply to public health measures in relation to the following categories of serious cross-border threats to health: (a) threats of biological origin, consisting of: (i) communicable diseases, including those of zoonotic origin; (ii) antimicrobial resistance and healthcare-associated infections related to communicable diseases (‘related special health issues’); (iii) biotoxins or other harmful biological agents not related to communicable diseases; (b) threats of chemical origin; (c) threats of environmental origin, including those due to the climate; (d) threats of unknown origin; and (e) events which may constitute public health emergencies of international concern under the International Health Regulations (IHR) (‘public health emergencies of international concern’), provided that they fall under one of the categories of threats set out in (a–d)

Term	Definition
	(Regulation (EU) 2022/2371, Article 2(1))
Statistics	'Statistics' means quantitative and qualitative, aggregated and representative information characterising a collective phenomenon in a considered population; (Regulation (EU) 223/2009, Article 3(1))
Synthetic data	Data that is artificially generated. The concept of synthetic data generation is to take an original data source (dataset) and create new, artificial data, with similar statistical properties from it.
Synthetic data documentation	Documentation of a synthetic dataset generated automatically or semi-automatically by the **synthetic data generator**. The documentation shall be anonymised so that it can be accompanied with the synthetic data set when released for the data user or for public use.
Synthetic data generator	A synthetic data generator is a software application, model or algorithm designed to generate **synthetic data**. It uses real-world data as input and generates a synthetic dataset. It is also possible to use parameters derived from the **original data** as input and/or modify additional parameters entered by the user.
Tabular data	Data organised in a structured format of rows and columns, where each row represents a single record or entity, and each column represents a specific attribute or variable. This structure is commonly found in spreadsheets or relational databases, making it easy to store, query, and analyse. Tabular data is often used for structured datasets where relationships between variables are well-defined.
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,

Term	Definition
	by the person lawfully in control of the information, to keep it secret. (Trade Secret Directive (2016/943), Article 2(1))
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; • 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 Regulation, Article 72 and Recital 76)
Trusted Research Environment (TRE)	TREs emerged from the UK health research sector, shaped by community-led principles and structured around flexible, function-based zones. They aim to create trusted, auditable access to sensitive data, often under national governance frameworks. TREs are not the same as Secure Processing Environments, which are legally defined in the EHDS Regulation.
Trusted third party (TTP)	A **pseudonymisation entity** which is independent from the data user and data holder that processes identifiers into pseudonyms. (ENISA, Pseudonymisation techniques and best practices). The TTP needs only to know the identifiers of the data

Term	Definition
	subjects on the basis of which it will compute the **pseudonyms**, and no other data. (EDPB Guideline 01/2025 Glossary, version adopted for public consultation)
Invoice	A legally binding commercial document, detailing the complete cost structure with breakdowns by services and data holders. It contains disaggregated cost elements, typically at the task level to favour clarity and transparency.
Request for payment	A formal request submitted to the data user for payment of the actual costs corresponding to work completed during a specific period. It follows the structure defined in the original invoice and refers to the relevant cost components outlined therein.
Payment instalment	One of several scheduled payments made in response to requests for payment. Each instalment corresponds to a portion of the total cost, aligned with the progress of the procedure or delivery of services
Payment	The financial transaction by which the user transfers the requested amount to the Health Data Access Body, Trusted Data Holder or the Data Holder in response to a request for payment.
Utility	Utility refers to how well the data supports its intended use, such as syntactical testing, analytical tasks, decision-making, or machine learning model performance. In the context of anonymised and synthetic data high utility means that insights, predictions, or outcomes derived from the data closely match those obtained using the **original data**.

Annex 5 Figure 1 enlarged

Overview of the applicant's mandate and the assessment of allowed purposes and prohibited secondary use of health data.