M8.1 Draft Guideline to Health Data Access Bodies "How to implement opt-out from secondary use of electronic health data"

TEHDAS2 –

Second Joint Action Towards the European Health Data Space

7 September 2025

Co-funded by the European Union

0 Document info

0.1 Authors

Lead Authors	Organisation
László Bencze	National Directorate General for Hospitals, Hungary
János Péter Misek	National Directorate General for Hospitals, Hungary
Irene Schlünder	TMF e.V., Germany
Roxana Albu	Sciensano, Belgium
Wannes Van Hoof	Sciensano, Belgium
Louise Mathieu	Sciensano, Belgium
Azul O’Flaherty	Department of Health, Ireland
Reviewers	
Asimina Boumpaki	Ministry of Health, Greece
Krisztina Davidovics	National Directorate General for Hospitals, Hungary
Krisztina Dienes-Horváth	National Directorate General for Hospitals, Hungary
Lorenz Dolanski-Aghamanoukjan	Gesundheit Österreich GmbH, Austria
Inge Franki	Health Data Agency, Belgium
Zdenek Gütter	Ministry of Health, Czech Republic
Csaba Kiss	National Directorate General for Hospitals, Hungary
Bart Motmans	Health Data Agency, Belgium
Maria Papaioannou	CYENS, Cyprus
András Pethő	National Directorate General for Hospitals, Hungary
Eva Zvirgzdiņa	Centre of Disease Prevention and Control of Latvia

0.2 Keywords

Keywords	TEHDAS2, Joint Action, Health Data, European Health Data Space, Health Data Access Body, Opt-out

0.3 Document history

Date	Version	Editor	Change	Status
05-5-2025	0.1	Authors and Contributors	First draft	Draft
19-6-2025	0.2	Authors and Contributors	Revisions and additions	Draft
20-6-2025	0.3	Authors and Contributors	Revisions according to EC review	Draft
3-7-2025	0.4	Authors and Contributors	Submission for internal review	Final draft
7-9-2025	0.5	EC review & Consortium review	Revised after internal review	Final
12-9-2025	1.0	Final version	Final version after PSG meeting	Final

Accepted in Project Steering Group on 12 September 2025.

Disclaimer

Copyright Notice

Table of Contents

1 Abbreviations

Term	Abbreviation
Data Governance Act	DGA
Data Protection Authorities	DPA
Electronic Identification, Authentication and trust Services	eIDAS
Electronic Health Record	EHR
European Data Protection Board	EDPB
European Health Data Space	EHDS
European Union	EU
European Union Agency for Cybersecurity	ENISA
General Data Protection Regulation	GDPR
Health Data Access Body	HDAB
International Electrotechnical Commission	IEC
International Organization for Standardization	ISO
Joint Action	JA
Member State	MS
Milestone	M
Secure Processing Environment	SPE
Trusted Third Party	TTP
Towards the European Health Data Space	TEHDAS
Work Package	WP

2 Executive summary

The overall objective of Task T.8.1 of the TEHDAS2 Joint action is to provide guidance to Health Data Access Bodies (HDABs) on their obligations under Article 71 of the European Health Data Space (EHDS) Regulation, regarding the right of natural persons to opt out from the secondary use of their personal electronic health data.

The primary audience of this guideline are HDABs, furthermore, some of the recommendations may also be useful to other stakeholders. It aims to provide HDABs with the necessary requirements and procedures to effectively implement and administer the opt-out mechanism, as well as advise them on ways they can engage citizens and foster public trust to enable data sharing for secondary use. OBJ nor to guide data users on how to manage data affected by this right.

The document outlines the main tasks and responsibilities of HDABs and gives recommendations for them in addressing opt-out based on the following legal and policy aspects:

- The definition of opt-out in secondary use [(Article 71 (1)], in contrast to opt-out in primary use [Article 10 (1)]. Certain important data protection issues are highlighted, with a focus on the difference between right to opt out, informed consent and the right to object, and the characteristics of personal electronic health data falling under opt-out, as well as the impact of opt-out on anonymisation.
- As regards the granularity of the opt-out, the guideline concludes that it is possible under the EHDS Regulation, falling under national competence. However, Member States are not obliged to introduce such a system.
- The guideline provides recommendations on the national mechanism of opt-out via centralised or decentralised national systems.
- The processing of electronic health data is discussed within the phases of data use before and after opt-out, and following the reversal of opt-out.
- The chapter on citizen engagement and empowerment provides recommendations on how to balance between respecting the rights of individuals and ensuring societal benefits, and how to foster public trust for the EHDS to be successful.

By using this guideline, HDABs will be better prepared to fulfil their responsibilities to natural persons regarding the opt-out from the secondary use of personal electronic health data under the EHDS Regulation. The guideline further helps to align national EHDS structures contributing to a harmonised approach to secondary use of health data across Europe. This document is part of a broader set of TEHDAS2 milestones aimed at supporting Member State readiness and promoting consistent EHDS implementation.

3 Introduction

As part of building 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 electronic health 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 electronic health data, and support data holders, data users and the new health data access bodies in fulfilling their responsibilities and obligations outlined in the Regulation.

TEHDAS2 focuses on several critical aspects of electronic health data use.

- Data discovery: Findability and availability of electronic health data, ensuring it is accessible for secondary purposes.
- Data access: Developing harmonised access procedures and establishing standardised approaches for granting electronic health data access across Member States.
- Secure processing environment: Defining technical specifications for environments where sensitive electronic 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 electronic health data is used.
- Collaboration models: Developing guidance on collaboration and guidelines on fees and penalties as well as third country and international access to electronic health 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 electronic health data, while also reducing fragmentation in policies and practices related to secondary use.

The primary focus of the work performed in Work Package 8 is on providing guidance to fulfil obligations towards natural persons and strengthening the engagement of citizens towards the EHDS regarding the secondary use of electronic health data. Task T8.1 addresses obligations towards natural persons through two milestone documents:

- M8.1 Draft guideline for Health Data Access Bodies on implementing opt-out
- M8.2 Draft guideline for Health Data Access Bodies on implementing the obligation of notifying the natural person on a significant finding from the secondary use of health data

This guideline provides HDABs with the necessary requirements and procedures to effectively implement and enforce the opt-out mechanism, as well as advise them on ways they can foster public trust to enable electronic health data sharing for secondary use. The guideline can also be used by other relevant stakeholders, especially trusted data holders.

Article 71 of the EHDS Regulation establishes a clear and enforceable right for all natural persons to opt out of the processing of their personal electronic health data for secondary use. This right applies across the EU and can be exercised at any time, without justification. It is reversible and must be made accessible and easily understandable.

While – like most rights and obligations under EU law - the right itself is established at EU level, its practical implementation is delegated to the Member States. This includes the responsibility to define the technical and procedural modalities of the opt-out mechanism and, where relevant, the conditions for narrowly defined exceptions as set out in Article 71(4).

In parallel, Article 10 of the EHDS Regulation allows Member States to provide, at national discretion, an opt-out mechanism from access to personal electronic health data for primary use — that is, for healthcare purposes — via national EHR systems.

The opt-out mechanisms for primary use and secondary use are distinct and independent from one another. A natural person may choose to exercise one without the other, and each must be implemented and managed separately in accordance with the respective provisions of the Regulation.[1]

This guideline covers the implementation of opt-out for **secondary use** of personal electronic health data.

[1] Recital (54) reflects the discussion.

4 Scope and aim of the guideline

This guideline covers **only** the implementation of opt-out for **secondary use** of personal electronic health data.

The scope is limited to the EHDS Regulation, and only referring to the GDPR insofar as it is explicitly complemented by the EHDS Regulation [Article 1(2)(a)]. This guideline does not attempt to interpret broader legal frameworks beyond what is necessary to implement Article 71. However, it is important to note that national law may supplement the Regulation where permitted [e.g., Article 71(4)]. No technical specifications can be provided here. The technical means to implement opt-out depend on many factors such as where opt-out is implemented: in a centralised or decentralised way, and how the right can be exercised: through different channels or through one entry point.

4.1 Audience

The primary audience of this guideline are HDABs. In addition, it can also inform data holders and trusted health data holders as far as they wish to learn to what extent they might be affected by the legal obligation to provide an opt-out mechanism. It is not meant to inform people about their opt out right. Neither is it intended to inform data users about the impact of the right to opt out on the result of data analysis. HDABs may draw on this guideline to inform how they deliver information duties under Articles 58–59 of the EHDS Regulation (together with TEHDAS guideline D8.3).

4.2 Legal framework

The EHDS Regulation does provide a Union-wide opt out right but does not provide for a Union-wide opt-out mechanism. Opt-out is to be implemented at Member State level and is applicable to personal electronic health data generated and held in that Member State.

It is the responsibility of national legislators to ensure that the right to opt out is implemented in a way that ensures compliance not only with the EHDS Regulation, but also with other laws. Among other applicable legal frameworks, the GDPR is particularly relevant. Pursuant to Article 1(2)(a) of the EHDS Regulation, the Regulation complements the rights laid down in the GDPR as regards the processing of personal electronic health data.

The rights of natural persons set out in the GDPR are unaffected. The supervisory authorities established pursuant to GDPR are competent for monitoring and enforcing the application of that Regulation, in particular for the monitoring of the processing of personal electronic health data and for handling any complaints lodged by the natural persons concerned. Article 21 of the GDPR states that the data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1) GDPR, including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

The EHDS Regulation defines a legal basis different from the consent mechanism under GDPR, where data processing begins e.g. after explicit individual agreement, the opt-out model introduced by the EHDS which creates a safeguard on which personal electronic health data may be used for secondary purposes by default, unless and until the data subject actively objects. The opt-out mechanism operates outside the actual process of data use — it is not a

prerequisite for data processing, but a safeguard designed to give individuals meaningful control over the inclusion of their data in secondary-use activities. In that sense, it functions more as a protective overlay than a procedural step, reinforcing individual autonomy without interrupting the legal grounds for data processing, such as those based on tasks in the public interest or legal obligations under Article 6(1)(c) or (e) GDPR.

The EHDS does not replace the GDPR; instead, it builds upon it by providing sector-specific governance, such as the establishment of HDABs, secure processing environments and structured data permits. While the GDPR allows for consent as one of several legal bases, it also permits national divergence in processing sensitive data under Article 9(4). The EHDS removes this divergence for secondary health data use by harmonising the process for access to data across Member States, except where stricter safeguards are introduced. Thus, the EHDS and GDPR operate in parallel: the former specifies and operationalises the latter's principles in the context of public health data governance, while the opt-out remains a supplementary rights-enhancing tool, not a substitute for legal justification.

Relationship between the legal basis and the opt-out

The right to opt out under the EHDS Regulation is independent from the legal basis under the GDPR.

The EHDS opt-out is sui generis right created by the EHDS Regulation, distinct from the GDPR right to object under Article 21 GDPR. It applies to the secondary use of health data under the EHDS legal framework and introduces a sector-specific mechanism allowing individuals to exclude their personal electronic health data from reuse, irrespective of the lawful basis under the GDPR. It is not an implementation or extension of Article 21 GDPR, but a complementary, autonomous instrument designed for the EHDS context.

The right to object under the GDPR is a general data protection right, allowing individuals to object to the processing of their personal data in specific circumstances, including direct marketing and processing based on legitimate interests. The right to opt out within the EHDS is a specific right related to health data, allowing individuals to object to the use of their health data for secondary purposes. The right to object in terms of the GDPR gives the data subject the right to object, on grounds relating to their particular situation, at any time to processing of their personal data when such processing is based on public interest [Article 6 (1)(e)] or legitimate interest [Article 6 para 1(f)]. After the objection the controller can no longer process the personal data unless it can demonstrate, compelling legitimate grounds which override the interests, rights and freedoms of the data subject. [Article 21 (1)] For scientific or historic research or statistical purposes, the right to object is valid unless the processing is necessary for the performance of a task carried out for reasons of public interest [Article (21)(6)] In other words, the data subject cannot exercise their right to object unless they give a personal reason to such objection and for scientific or statistical use this is not enough if the processing is necessary for public interest reasons. The right to object is thus conditioned by disclosing personal reasons by the data subject, that is more personal data, and the eventual overriding interests of the controller.

In conclusion:

- The GDPR is the foundation, while the EHDS Regulation builds on it for health-specific scenarios.
- The EHDS Regulation introduces real-time digital rights, especially for primary use access, which go beyond GDPR’s manual processes.

- For secondary use, the EHDS Regulation defines structured legal bases, processing rules, and governance mechanisms (including those implemented through tasks assigned to HDABs), in alignment with GDPR.

Table 1 Summary of the relationship between the EHDS Regulation and GDPR (question 56, European Commission FAQ 5th March 2025)

Aspect	GDPR	EHDS Regulation
Legal role	Core legal framework for data protection in the EU	Sector-specific complement focused on health data
Main focus	Sets out rights for individuals and obligations for data controllers/processors	Adds specific provisions for the use, access, and reuse of electronic health data
Supervisory Authorities	Data Protection Authorities (DPAs) monitor GDPR compliance (Lawfulness of processing in general)	Same DPAs also monitor EHDS implementation
Right of Access (General)	Individuals can request access to all personal data held by a controller (Article 15 GDPR)	Individuals have immediate access to specific electronic health data (e.g. patient summary) via self-service
Time to Respond to Access Request	Up to 1 month; can refuse or charge for repetitive/unfounded requests	Immediate access required; no refusal or fees allowed, regardless of frequency
Primary Use of Data	GDPR applies; access requests must be processed manually	EHDS adds real-time, digital access to essential health data
Legal Basis for Processing	Must rely on one of the legal bases under Article 6(1) GDPR	EHDS establishes legal bases: Article 6(1)(e) (task in public interest) for HDABs and Article 6(1)(c) for data holders
Processing Special Categories	Processing health data only allowed under Article 9(2) with safeguards	EHDS provides lawful grounds and safeguards (e.g., secure processing, data permits – Chapter IV)
Secondary Use of Data	Not specifically regulated by GDPR	Structured access for **secondary use** governed by HDABs, permits, secure environments
Safeguards for Sensitive Data	Requires implementation of **appropriate safeguards** (Article 9(2)(j))	EHDS includes legally binding safeguards in Chapter IV

It is important to highlight that, while according to Article 9(4) of the GDPR, Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health. While under the EHDS Member States cannot introduce further consent rules, except for stricter safeguards.

However, the right to opt out under Article 71 EHDS is a separate, EHDS-specific right, to be implemented and managed by HDABs. In the framework of contact with supervisory authorities pursuant to GDPR, the Article 65 of the EHDS Regulation states, these supervisory authority or authorities shall also be competent for monitoring and enforcing the application of the right to opt out from the processing of personal electronic health data for secondary use pursuant to Article 71, and in this context these authorities shall be empowered to impose administrative fines up to the amount referred to in GDPR. If a Member State has provided for the right to opt out pursuant to Article 71 to be exercised through the HDABs, the relevant HDABs shall provide public information about the procedure to opt out and facilitate the exercise of that right [Article 58 (2)].

When implementing the opt-out mechanism at Member State level, particular attention should be paid to the following aspects:

- role, tasks and obligations of HDABs and of (trusted) data holders
- information systems to record, store, manage, check and respect the opt-out decisions of individuals
- centralised or decentralised systems to manage the opt-out mechanism, and how it is coordinated between HDABs and data holders
- whether, and under which national conditions, exceptions to the opt out right may be applied in accordance with Article 71(4)
- The possible granularity of the opt-out mechanism (e.g., full opt-out from all secondary uses or selective exclusion of specific data categories or purposes).

This guideline supports HDABs in implementing these elements in a manner that respects natural person’s fundamental rights, ensures legal compliance, and maintains trust in the EHDS framework.

5 Right to opt out from the processing of personal electronic health data for secondary use

5.1 What is opt-out? Definition.

5.1.1 Legal definition

Article 71 of the EHDS Regulation obliges Member States to establish an opt-out mechanism for the secondary use of personal electronic health data. Article 71(1) of the EHDS Regulation states: “Natural persons shall have the right to opt out at any time, and without providing any reason, from the processing of personal electronic health data relating to them for secondary use under this Regulation. The exercise of that right shall be reversible.” This right is unconditional and reversible.

An important element of this provision is that individuals can exercise their right without providing any reason. The mere declaration to not share their data for secondary use, partially or in whole, is sufficient. They can do so at any time; the right is not limited in time and there is no deadline to meet.

5.1.2 Opt-out from secondary use in contrast to opt out from primary use

5.1.2.1 Legal Requirements by the Regulation

Article 10 of the EHDS Regulation allows Member States the option to provide natural persons the right to opt out from the access to their health data as set up under the EHDS Regulation for primary use. There is no automatic link between opting out in primary or secondary use. It is possible for a natural person to use one opt-out right, but not the other.

The right to restrict access according to Article 8 of the EHDS Regulation allows natural persons to limit the visibility of certain parts of their electronic health data. This restriction is limited to the visibility of data in an EHR by healthcare professionals using the health professional access services referred to in Article 12. It does not follow that these restricted data are unavailable for secondary purposes, even where the EHR is the data source. Where electronic health data that has been restricted in this way are requested through the HDAB for secondary purposes, those data will be available. Therefore, there is no relationship between the right to restrict access and secondary purposes. If a natural person does not want these electronic health data to be accessed for secondary use, they need to also opt-out in accordance with Article 71.

5.1.2.2 Recommended good practice

It is recommended that HDABs inform individuals that primary and secondary use opt-outs are distinct choices. HDABs should clearly explain how electronic health data can be blocked for medical exchange but still reused in pseudonymised format for secondary use.

5.1.3 Difference between EHDS opt-out, and GDPR informed consent and right to object

Informed consent requires obtaining explicit permission from individuals before their data can be used. It is a cornerstone of ethical data use, ensuring individuals are fully aware of how their data will be used and the implications. Article 4 (11) of the GDPR contains the official definition of “consent”. It specifies that consent must be voluntary, specific, informed, and unambiguous. This is key to understanding the “informed” part.

The Article 6 (1) of the GDPR lists the legal bases on which personal data may be lawfully processed. According to point (a), processing is lawful if “the data subject has given consent to the processing of his or her personal data for one or more specific purposes.” This is therefore consent as a legal basis.

The Article 7 of the GDPR sets out the conditions for consent. It specifies that:

- The controller must be able to demonstrate that the data subject has consented to the processing,
- Consent must be given separately from other statements and must be easily accessible, clear, and written in simple language,
- The data subject has the right to withdraw their consent at any time.

The main difference between opt-out in the EHDS Regulation and the right to object under Article 21 of the GDPR is that no justification is required for the exercise of the right to opt out in EHDS. The right to object under the GDPR is a general data protection right not limited to electronic health data like in the EHDS. It allows individuals to object to the processing of their personal data in specific circumstances, including direct marketing and processing based on legitimate interests. The right to opt out within the EHDS is a specific right related to electronic health data, allowing individuals to opt out from the re-use of their electronic health data for primary and secondary purposes within the EHDS framework. It is important to highlight that EHDS opt-out does not require a justification and cannot be overridden by the controller, unlike Article 21 GDPR.

GDPR gives the data subject the right to object, on grounds relating to their particular situation (as GDPR requires the data subject to provide reasons relating to their specific situation) at any time to processing of their personal data when such processing is based on public interest [Article 6 (1)(e)] or legitimate interest [Article 6 (1)(f)]. After the objection, the controller shall no longer process the personal data unless the controller demonstrates the existence of compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims [Article 21 (1)]. For scientific or historic research or statistical purposes the right to object is valid unless the processing is necessary for the performance of a task carried out for reasons of public interest [Article 21 (6)]. In other words, the data subject cannot exercise their right to object unless they give a personal reason to such objection and for scientific or statistical use this may not be enough if the processing is deemed to be necessary for public interest reasons. Right to object is thus conditioned by disclosing personal reasons by the data subject and can be overridden by the compelling interests of the controller.The right to object and the right to opt out are thus cumulative and independent. The exercise of the GDPR right to object does not automatically trigger an EHDS opt-out, nor does an EHDS opt-out preclude the individual from also exercising their GDPR right to object to processing. Controllers must respect both decisions separately and ensure that both objections and opt-outs are recorded and implemented appropriately, according to their respective legal bases and effects.

The EHDS Regulation establishes specific information mechanisms, such as the public information portal (see Guideline Task 8.2. Informing natural persons about the use of health data – “Citizen Information Point”). This is intended to provide continuous, accessible updates about the purposes, recipients, and outcomes of secondary data use within the EHDS infrastructure.

The EHDS Regulation does not impose an obligation to individually notify data subjects, including those whose data were initially collected on the basis of informed consent. However, under Article 14 GDPR, general transparency obligations still apply and should be fulfilled through public notices and accessible documentation.

5.1.4 Citizen engagement and empowerment as regards the opt-out

The EHDS Regulation requires Member States to set up an opt-out mechanism regarding the secondary use of personal health data in order to protect data subjects' right to respect for their autonomy. However, its use might hinder the overall goal of the EHDS, i.e. to realize societal benefits, e.g., a bias in the datasets and in the data processing results could affect the utility and precision of secondary data use. To balance between societal benefits of the secondary use of health data and the opt out right as a guarantee, this chapter aims at contextualising the opt-out mechanism within the overall goal of the secondary use of health data, and guide HDABs on how to ensure an implementation of the EHDS framework that is trustworthy and respects individual rights.

The necessity to preserve the right for the autonomy of natural persons is explained in Recital 54 of the EHDS, which provides that "to balance the need of health data users to have exhaustive and representative datasets with the need for autonomy of natural persons over personal electronic health data of theirs that are considered particularly sensitive, natural persons should be able to make the decision as to whether their personal electronic health data can be processed for secondary use under this Regulation, in the form of a right to opt out from having those data being made available for secondary use". This opt-out mechanism is embedded in Article 71 of the EHDS Regulation. Importantly, while this mechanism allows individuals to exclude their identifiable data from secondary use, it is designed in a way that still enables the creation of large, representative datasets for societal benefit, such as research, innovation, and policy.

5.1.4.1 Societal benefits as the justification for secondary use

From the outset, the Regulation frames secondary use as a mean to unlock the societal value of electronic health data, particularly in enhancing health systems and services across the Union. As mentioned early on in the first recital of the Regulation, the aim of the EHDS regarding secondary use is "*to better achieve other purposes involving the use of electronic health data in the healthcare and care sectors that would benefit society (…)".* As provided in further parts of the text, access to data for secondary use is therefore both encouraged and conditional to "*contribute to the general interest of society"*. Furthermore, when describing the different purposes for which health data can be used for secondary purposes, Article 53 states that scientific research related to health or care sectors can be conducted "*with the aim of benefiting end-users, such as patients, health professionals and health administrators (…)"*. As the opt-out mechanism does not trigger or initiate the process of secondary use of health data but instead serves as a critical safeguard – an exit route for individuals who wish to withdraw their data – it cannot be viewed as the justification for such processing. Rather, the justification for secondary use lies in the legitimate societal benefits it is intended to generate, such as improved public health, research, innovation, and evidence-based policymaking. These benefits provide the normative and legal grounds upon which secondary use is structured. In this context, the opt-out mechanism functions not as a form of presumed consent, but as a protective measure to uphold individual autonomy within a system that enables data use by default.

The opt-out mechanism is not a form of consent or engagement, but a fundamental safeguard to protect autonomy. Its use reflects the need for trust in the EHDS secondary use system, which must be robust and respectful of individual rights. Therefore, the EHDS framework relies on that the process of secondary use of health data it will implement is trustworthy and safe enough so that the opt-out mechanism remains a last resort safety valve.

5.1.4.2 Top-down channels: from the HDABs to the public:

The HDABs bear a crucial responsibility under the EHDS framework to ensure that ethical, legal, and social considerations are fully integrated into the governance of secondary use. This means not only complying with legal requirements but proactively engaging with the public to ensure that citizens are fully informed about both the benefits and the potential implications of allowing their electronic health data to be reused. This is particularly the case regarding who can access data, for what purposes, and under what safeguards. The success and sustainability of the EHDS depends on making secondary data use the norm rather than the exception, but this can only be achieved through transparency, trust, and mutual understanding.

5.1.4.3 Promoting awareness of societal benefits

Article 58(2) requires HDABs to inform the public about which entities accessed which datasets, for which purposes, and with what outcomes. This information should be used not only to comply, but to demonstrate societal benefit clearly and continuously.2 Information could be both a passive way of engaging the public, while providing insights on what societal benefits are realised and how their achievement could be affected when exercising opt out. Indeed, for instance, the HDABs' duty to inform includes to provide insights on what benefits have been realised and by whom since the information provided to data subjects will have to cover, among other aspects, "who has been granted access to datasets of electronic health data and to which datasets they were granted access and details of the data permit regarding the purposes for processing such data as referred to in Article 53(1)" as well as "the results or outcomes of the projects for which the electronic health data were used.". Even though it could be difficult to understand prior of the EHDS implementation all the factors that could drive the activation of an opt-out mechanism, HDABs can play a key role in ensuring natural persons do not do so as a result of a lack of understanding of the process and benefits of the secondary use of health data. By focusing on how societal benefits are realised, natural persons can grasp how data from each individual is relevant to achieve societal benefits.

It is recommended to inform citizens on the purposes for which data is processed (e.g., public interest, policy support and scientific research) and that opt-out may limit the usefulness of this data processing. By engaging effectively, the HDAB enables persons to make informed decisions about their opt-out choice. To properly support this, information about secondary use should be balanced and also acknowledge any risks or drawbacks.

5.1.4.4 Digital health literacy, digital health access and diversify communication channels:

However, it is worth noting that digital health literacy can vary significantly among groups of populations and among individuals. Communication channels and formats should be adapted accordingly to adjust to this reality. In that vein, it can be interesting to remember that the EHDS Regulation also requires Member states to conduct awareness-raising initiatives to inform the public about the secondary use of health data and the EHDS framework, including "the advantages, risks and potential gains for science and society of primary use and secondary use". Furthermore, Article 84 (2) of the EHDS stipulating that such initiatives shall be "tailored to the needs of specific groups and shall be developed, reviewed and, where necessary, updated".

Following up on HDABs advances and above all learning from how they assessed and address the varying degrees of literacy among the population and hence the different needs and levels of attention required for certain vulnerable groups could be useful to make sure the adequate

[2] The information portal will be discussed in Milestone M8.3.

formats and channels are provided for different population groups so they can properly be engaged in the secondary use of health data.

5.1.4.5 Bottom-up channels - from the public to HDABs:

Effective engagement can ensure that natural persons do not opt out due to lack of understanding of the benefits of sharing health data for secondary purposes. However, it is worth noting that societal benefits is a concept that remains largely undefined. Understandably, defining such a concept at the European level might be irrelevant, as it will apply in culturally different societies.

It is then essential to realise that the implementation of the EHDS at national and sub-national level of the secondary use of health data is an exercise that will determine the nature of these societal benefits. In practice, HDABs influence how societal benefit is interpreted at national level, through the applications they authorize. They should engage stakeholders to ensure these interpretations reflect ethical, cultural, and public expectations.

Indeed, surveys and public consultations across the EU reveal that people are more likely to support the secondary use of their health data when they are involved in discussions around purpose, safeguards, and oversight.

5.1.4.6 Collaborating and learning from stakeholders

Within the EHDS, the effectiveness of cooperation between parties is facilitated by participatory and responsive implementation processes, as well as by ensuring transparency, accountability, and public involvement in the governance of health data. Cooperation between the various stakeholders is supported by particularly the following regulations:

I. Stakeholder engagement (Articles 57 and 59 EHDS)

EHDS Regulation establishes mechanisms to ensure that HDABs engage meaningfully with stakeholders. According to Article 57, HDABs are required to “cooperate with all relevant stakeholders, including patient organisations, representatives of natural persons, health professionals, researchers, and ethics committees, where applicable in accordance with Union or national law.” While the regulation does not impose specific modalities or procedures for this cooperation, it creates space for HDABs to engage with these groups in ways that reflect social expectations and ethical standards regarding the secondary use of health data. Such engagement is essential for building public trust and for understanding what is considered socially acceptable in terms of data access and reuse.

II. EHDS Stakeholder Forum (Articles 93 EHDS)

In addition to the above, the EHDS Regulation establishes a Stakeholder Forum under Article 93 (1), designed “to facilitate the exchange of information and promote cooperation among stakeholders in relation to the implementation of this Regulation.” According to Artice 93 (2) the stakeholder forum shall be composed of relevant stakeholders, including representatives of patient organisations, health professionals, industry, consumer organisations, scientific researchers and academia, and shall represent their views, and the tasks of the stakeholder forum shall encompass equally primary use and secondary use. The Stakeholder Forum has an advisory function to the EHDS Board, whose role is to ensure coordination between Member States and the European Commission (Article 92 (1)).

5.1.4.7 Co-building a data culture:

HDABS have an obligation to cooperate with relevant stakeholders during the exercise of their tasks. (Article 57). However, this should be understood as a minimum requirement rather than a complete model for public engagement. Other initiatives may be taken at the will of these bodies and their respective Member States and should be encouraged to complement these cooperative efforts and promote public trust in the secondary use of health data.

To foster trust, HDABS should:

- Inform the public clearly about the societal benefits and safeguards of secondary use;
- Involve stakeholders who can represent the views of natural persons;
- Where appropriate, engage directly with citizens or build on existing public participation initiatives.

Insight into public views can help to build trust as well as to understand what such trust us dependent upon. These views can be taken into account in the process of the secondary use of health data in order for HDABs to understand how the public understands societal benefits and what data use means to them at a societal level, as well as to ensure that the EHDS implementation aligns as much as possible with these perspectives, to ensure its trustworthiness and resulting success.[3]

5.2 Opt-out from what

5.2.1 Characteristics of data falling under the opt-out

5.2.1.1 Legal Requirements by the Regulation

Natural persons can opt out from secondary use of their own personal electronic health data. The opt-out applies only to their personal electronic health data (directly and indirectly identifiable or re-identifiable - if a health data holder can identify a natural person in a dataset it holds).

Article 71(8) EHDS Regulation states: “When the purposes of the processing of personal electronic health data by a health data holder do not or no longer require the identification of a data subject by the controller, that health data holder shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with the right to opt out under this Article.”

5.2.1.2 Limits of the opt-out mechanism:

The EHDS introduces narrowly defined exceptions to the right to opt out in Article 71(4). Member States may adopt national laws allowing access to health data of individuals who have opted out, provided that three cumulative conditions are met:

1. The application or request is made by a public sector body, Union institution, carrying out tasks in the area of public health, or on behalf of such an entity, and

The data is necessary for public health purposes (i.e., those listed in Article 53(1)(a)-(c)) or for scientific research for important reasons of public interest.

[3] Such an initiative was carried out in the European Joint Action TEHDAS. Between 2021 and 2023, citizens from different European countries participated in the online Healthy Data Consultation to express their views on the secondary use of health data and how they wish to be engaged in it.

2. The data cannot be obtained by alternative means in a timely and effective manner under equivalent conditions.

3. The applicant has provided sufficient justification why data for which a right to opt out has been exercised should be made available.

Such a mechanism can be provided for in national law and must include specific and appropriate safeguards to protect the rights and freedoms of natural persons. These include the prohibition of re-identification [Article 61(3)], the use of secure processing environments [Chapter IV], and the respect of necessity and proportionality in a democratic society [Article 71(5)-(6)].

Regarding the legal capacity required in relation to the contents of this guideline, regulations are made in each Member State. Pragmatically the opt-out status set by legal guardians remains unchanged even after reaching the age of majority.

5.2.1.3 National discretion

In terms of how a person whose legal capacity is affected (e.g. minor, person with limited legal capacity, person under guardianship) can exercise the right to opt-out, the legislation of each Member State may lead to different results. In any case, it is worth noting as a basic principle that in the event of gaining/regaining the appropriate legal capacity, the data subject should be granted the right to decide (also in the case of exercising the right to opt-out – e.g. optimally supported a message about the opportunity of setting, changing the status).

5.2.2 Does opt-out block anonymisation?

The opt-out also applies to the processing of personal data for the purpose of answering data requests. It is important to note that although the final output of the data request will be non-personal, generating that output may require the processing of personal data. This is not possible after opting out.

5.2.2.1 Legal Requirements by the Regulation

Under the GDPR, the term processing is defined very broadly in Article 4(2) to include any operation performed on personal data including collection, storage, adaptation, use, disclosure, and anonymisation. While anonymised data is no longer considered “personal data” under the GDPR (Recital 26), the act of anonymising data still constitutes processing if it is applied to identifiable data. Hence, anonymisation requires a legal basis, and the controller is subject to the GDPR for such processing activity.

In the context of the EHDS Regulation, Article 71(1) and (3) provides individuals with the right to opt-out of having their health data made available for secondary use under the EHDS Regulation, which explicitly includes data that is still personal at the time of processing. This would therefore also include processing activities that aim to anonymise or pseudonymise the data to make them available through the EHDS for secondary use. This strict interpretation reinforces the notion that the opt-out right applies not just to the use of the electronic health data but to the entire chain of processing activities related to secondary use under the EHDS framework. This requirement does not apply to datasets that were already anonymised (personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable) before the individual exercised their opt-out right.

5.2.3 Are there different levels of opt-out available in EHDS?

5.2.3.1 National discretion

Member States retain the flexibility to design and implement the opt-out mechanism with as much granularity as they deem appropriate. The EHDS Regulation leaves the level of opt-out granularity to Member States, without imposing any obligation in this regard. Member States may provide the option, for example, to allow individuals to opt out of specific types of secondary use or individual data categories. However, excessive complexity can create significant administrative burdens and may risk undermining the overall coherence and interoperability of the EHDS framework. Greater granularity may enhance individual control, but it also increases the effort required to ensure EHDS compliance, system transparency, and usability. Therefore, it is recommended that Member States focus on defining a limited set of essential, meaningful opt-out levels — those that reflect real differences in data sensitivity and public expectations, naturally if a Member State chooses for granular opt-out. Of course, it is important to point out three general characteristics related to these levels in this document. First of all, the resulting stratification must be legally manageable in some way, and it is also necessary to designate levels that are technically feasible. In addition to the above, it is very important that the regulations to be developed and the feasible technical options are socially acceptable.

5.2.3.2 Recommended good practice

However, what opt-out levels constitute “essential” may vary across jurisdictions, often shaped by cultural norms, legal traditions, and the extent of individual autonomy typically granted in health-related decision-making. In designing these systems, policymakers must carefully balance personalisation and practicality: too little granularity may erode trust, while too much may lead to confusion, decision fatigue, and low engagement.

Crucially, as health data flows increasingly across borders there is a growing need to align opt-out frameworks across the EU, ensuring they are interoperable, transparent, and intelligible not only to institutions but also to individuals. This also means aligning with international standards to facilitate secure and ethical data sharing beyond the EU. In this context, it becomes essential to design opt-out mechanisms that are citizen-centred but not burdensome, allowing individuals to exercise control informedly and reflectively, without being overwhelmed by fragmented or overly technical choices. Only by achieving this balance can the EHDS foster sustainable, trusted cross-border collaboration while respecting fundamental rights.

It is recommended that HDABs inform individuals that opt-outs do not propagate automatically across borders, and citizens may need to submit opt-outs for their data stored in each relevant country. HDABs could suggest alignment efforts as a future policy recommendation to improve citizen-friendliness. It is also recommended that Member States use suitable rules, measures, and tools (e.g. information portals) to help citizens obtain information, make decisions, and collect and provide the necessary data.

While not required, granular opt-out mechanisms (e.g., by data type or purpose) may be a best practice if technically feasible and proportionate. However, the level of granularity generally increases the organisational effort and possibly also the effort required to make the system EHDS-compliant. It is therefore advisable to only map essential levels. Which these are can vary from state to state and often depends on the degree of decision-making freedom that is customary in the respective cultural background.

When considering a granular opt-out mechanism, it is recommended to distinguish meaningful and manageable levels, such as:

- full opt-out,
- opt-out for specific data types, e.g. genomic data, images,
- per data holder, e.g., cohorts, biobanks, EHR,
- per purpose of data use, e.g., research, innovation, policy development.

In summary:

- **Granuar opt-out is possible** but not required under EHDS.
- Member States can implement **granular mechanisms**, but must weigh **usability, EHDS compliance**, and **cross-border interoperability** (e.g. national differences in stratification, comparability of data sets).
- The system must avoid **resembling consent-based logic**, as the EHDS is not built on informed consent.
- **A well-balanced design,** perhaps offering 2–3 meaningful layers, can preserve individual choice while supporting public trust and societal benefit.
- Alignment across Member States should be a key consideration to avoid fragmentation undermining access to data for secondary use on European level.

5.3 Where to declare opt-out

5.3.1 Role of the HDABs and the opt-out

5.3.1.1 Legal Requirements by the Regulation

The EHDS Regulation assigns HDABs a central role in governing secondary use of electronic health data. However, based on national implementation choices, the data holders also may functioning as a possible point of contact[4]. It ultimately leaves it to each Member State to determine how responsibilities for implementing the opt-out mechanism are allocated, including which entity serves – maybe as the primary contact point - for individuals exercising their rights.

National discretion

Example of possible step-by-step Chain of Responsibility:

1. Initiation by the Individual:
   The data subject initiates an opt-out request via a channel established by the Member State e.g. a national opt-out portal, their healthcare provider, national EHR portal, or eHealth application.
2. Identity Verification (GDPR-compliant):
   Identity verification is performed through channels designated by the Member State (e.g., healthcare provider, data holder, or central system), using secure and GDPR-compliant mechanisms. It is also worth considering Member States the use of provisions and tools for electronic identification and trust services, which can be particularly effective in cross-border data flows. Based on examples such as eiDAS Regulation demonstrate, a potential system can be created that allows the parties

[4] See Article 71 (8) of the EHDS Regulation: "When the purposes of the processing of personal electronic health data by a **health data holder** do not or no longer require the identification of a data subject by the controller, that **health data holder** shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with the right to opt out under this Article."

involved to communicate with each other securely and smoothly, breaking down technical and legal barriers between different Member States.

3. Transmission to HDAB (Within the framework of Article 71(2) of the EHDS Regulation): The opt-out status is relayed securely to an opt-out database or registry. The MS may decide whether this is housed at the HDAB or at another national entity.
4. User Confirmation and Transparency (GDPR Articles 15 EHDS Articles 58, 71): The individual receives a confirmation receipt and can view their status and previous decisions. Based on MS legislation, it can be managed via a centralised public information portal maintained or coordinated by the HDAB or managed in a decentralised way by the data holders.

In case of more than one HDAB per country, Member States should ensure coordination mechanisms are in place to prevent fragmentation and ensure consistency in opt-out application across all HDABs and data holders. Possible approaches may include the primary competence of a coordinating HDAB or the sharing of competence between HDABs, or a decentralised management at the level of data holders.

Possible role and responsibilities of Data Holders:

- Data holders, where designated, must respect opt-out statuses communicated via HDABs or other competent authorities and ensure no processing takes place for secondary use purposes where such an opt-out is in effect.
- Before making data available data holders are also responsible for ensuring that health data they manage comply with the individuals' opt-out decisions.

5.4 How to declare opt-out

5.4.1 Legal requires by the Regulation

According to Article 71(2) of the EHDS Regulation: “Member States shall provide for an accessible and easily understandable opt-out mechanism to exercise the right established in paragraph 1, whereby natural persons may explicitly state that they do not wish to have their personal electronic health data processed for secondary use”.

5.4.1.1 National discretion

Principles recommended to follow are:

- Member States must ensure that the opt-out mechanism is non-discriminatory and inclusive, covering the needs of diverse population groups.
- Digital-first approaches (e.g., national EHR portals, eHealth apps) can be efficient, but alternative channels (e.g., paper-based forms, in-person declarations via healthcare providers) must be considered for citizens with limited digital access or literacy.
- Accessibility also includes language, disability, and cognitive comprehension. The opt-out interface should comply with national language requirements as well as accessibility standards The opt-out interface should comply with national language requirements as well as accessibility standards (e.g., WCAG) i.e. Web Content Accessibility Guidelines (WCAG) version 2.0 or above. The interface should meet applicable requirements originating from the Web Accessibility Directive and Harmonised European Standard Harmonised on Accessibility.
- Member States must provide clear, plain-language explanations of what the opt-out does and does not do. These explanations should include that it applies only to secondary use under the EHDS, does not affect primary care, access to services, or

the existence of the EHR, and that is reversible at any time. Explanations should avoid technical or legal jargon and could use visuals or infographics, where helpful.

- If granular opt-out is offered, each level must be clearly defined and distinguishable with meaningful choices, and of course they must also be operationally enforceable.
- Ensure distinction from other rights (e.g., opt-out for primary use, right to restrict access under Article 8) is clearly explained and communicated.
- Opt-out implemented by (university) hospitals, and centralised, if necessary.

5.4.1.2 Recommended good practice

In practical terms, at the current stage of the implementation of the EHDS Regulation, only a few examples could be listed as possible recommendations to consider by Member States, as follows:

- Deployment of an online portal where people can make their opt-out choice. Such a portal may be co-located with the national EHR, if applicable. It would mean that individuals could apply all their decisions related to EHDS in one place.
- Alternatively, and opt out mechanism may be a dedicated portal hosted by the HDAB(s) or the coordinating HDAB, if applicable, meaning more cohesion with secondary use.
- Interaction with health data holders or healthcare professionals may also be an option but it may cause difficulties with accessibility, and it could increase the administrative burden on the healthcare system. However, it might also be an alternative for people with limited digital literacy.
- Other one-stop shop solutions, e.g., (local) government offices.
- Any combination of the above-mentioned solutions of further options.
- Engage citizens in the design process to ensure understandability.

5.4.2 Data protection aspects of declaring and reversing opt-out

5.4.2.1 Legal Requirements by the Regulation

Opt-out registry – keep tracking of opt-out decisions

From registry to data blocking: The exercise of the opt-out right under Article 71 of the EHDS Regulation could entail privacy risks, particularly regarding how opt-out declarations are recorded, stored, and acted upon. The process must ensure that individuals can exercise control over the secondary use of their electronic health data without exposing themselves to additional personal data risks.

Revoking opt-out: restoring availability

The opt-out must be reversible at any time, as stated in Article 71(1). Reversal applies only to data permits or requests authorised after the revocation [Article 71(3)]. Revocation must:

- Be as simple and accessible as the initial opt-out.
- Trigger automatic update of the registry and downstream systems.
- Be reflected immediately in any future secondary use authorisations, though it does not affect past data uses approved before the reversal [EHDS Article 71(3)].

To prevent misuse or ambiguity, the system should require identity confirmation before reversal is accepted.

5.4.2.2 National discretion

Opt-out Registry: Declaring the Decision

To manage and enforce opt-outs consistently across the Union, Member States or designated HDABs can maintain a secure opt-out registry. This registry should:

- Record only necessary data to identify the individual and confirm the opt-out status (in line with GDPR Article 5(1)(c) – data minimisation).
- Purpose limitation: any processing must remain strictly limited to purposes compatible with the registry’s function (e.g., verifying opt-out status), and not extend to recontact or analytics unless expressly authorised by law.
- Use pseudonymised or encrypted identifiers wherever possible to reduce re-identification risk.
- Ensure data subject authentication is robust, possibly via EU digital identification options (eiDAS) / national digital ID or healthcare credentials, to confirm whom an opt-out relates to.

The registry must also:

- Provide immediate confirmation of opt-out status to the individual.
- Log the timestamp and source of the declaration.
- Be accessible (via national portal or HDAB interface) so the individual can view, update, or revoke their declaration easily.
- Security and access controls: registry access must be limited to authorised entities with a clearly defined role (e.g., HDABs or designated public authorities) and subject to logging and oversight.

Maintaining a centralised list of opted-out individuals: it requires particular attention under data protection law, as such registries may — if not properly safeguarded — reveal sensitive individual choices. Member States must ensure this information is processed strictly within the legal purpose and is protected from unauthorised inference or secondary use. Maintaining an opt-out registry is only the first step. The real safeguard lies in ensuring the registry is technically and legally connected to downstream systems so that:

- Opted out individuals’ data shall be excluded from any new data permits or health data requests - subject to the exceptional cases referred to in Article 71 (4). It may be carried out at dataset, data holder, or HDAB level, as implemented by the Member State.
- Data holders (e.g., hospitals, registries) are notified of opt-out status and ensure that relevant electronic health data is not transferred or made available for secondary use.
- If applicable, sensitive data (Recital 17) marked for blocking at the source is handled directly, ideally using EHR-level tagging that prevents sharing. It may be carried out at dataset or data holder level, as implemented by the Member State.
- This requires interoperable technical standards, national integration with the EHDS infrastructure, and strong governance protocols.

In summary, data filtering can basically be done:

- At the data holder level: This is the first and most important filtering point. As soon as the user exercises their opt-out right, healthcare data controllers (e.g., hospitals, clinics, medical records) must be notified immediately. They must ensure that the data concerned is not transferred for secondary use (e.g. for research or statistical purposes). This filtering takes place at the source, minimizing the risk.
- At the dataset level: Here, data filtering takes place at a higher, more aggregated level. When a researcher or organization submits a data request, the system releasing the data must put in place a technical barrier to prevent the release of data with opt-out status. This is a secondary line of defence that filters out non-transferable data from the entire dataset.

5.5 How to implement opt-out with regard to citizens' rights

5.5.1 How to inform citizens about their right to opt out?

The rules for informing citizens are set out in Article 58(1) of the EHDS Regulation which stipulates that HDABs shall make information on the conditions under which electronic health data for secondary use are made publicly available, easily searchable through electronic means and accessible for natural persons.

In the present guideline, information to citizens is discussed in general terms in the chapter on Citizen engagement and empowerment as regards the opt-out. The information portal for citizens will be addressed in detail by milestone M8.3.

Before individuals can meaningfully exercise their right to opt out from the secondary use of their health data, they must be clearly and proactively informed of that right. HDABs play a central role in this process. Under the EHDS Regulation, HDABs have specific legal duties when they are entrusted with managing the opt-out mechanism. In addition, HDABs may voluntarily take on broader communication and support functions to strengthen transparency and public trust. HDABs ensure electronic transparency tools, as they are required to maintain a publicly available and electronically searchable register that shows information on data permits, categories of data used, identities of data users, the legal basis for access, and applicable safeguards. This transparency supports accountability and helps build trust in the secondary use system.

This section outlines, first, what HDABs must do by law, and second, what they may choose to do as part of a wider role as an information hub.

5.5.1.1 Requirements by the Regulation

Mandatory public information
If a Member State has provided for the right to opt out pursuant to Article 71 of the EHDS Regulation to be exercised through the health data access bodies, the HDAB is legally required to provide public information about the procedure to opt out. This includes clear instructions, available formats, and access points that enable natural persons to exercise their right. However, the general requirement on the opt-out mechanism in Article 71 of EHDS Regulation is that it must be 'accessible', which also means that there must be public information about its existence, so it means, if this right is exercised elsewhere, it's for Member States to ensure sufficient publicity.

Facilitation of the opt-out process
The obligation to provide an opt-out mechanism is on Member States as whole. If they may decide to assign this to health data access bodies, the HDABs must also ensure that the opt-out mechanism is effectively in place and can be used by individuals. While they are not necessarily required to operate the system themselves, they are responsible for making sure

that the opt-out process is clearly defined, accessible, and easy to understand for all users — including people with disabilities and those with limited digital skills. It is important to clarify, that these obligations only apply to HBABs only if they are responsible to implement the opt out - otherwise the responsibility lies with the Member State.

Reporting duties
HDABs must publish activity reports every two years. These must include data on permit applications, granted and refused permits, categories of data used, types of applicants, and decisions on exceptional access under article 71(4), including the number of data permit decisions involving individuals who opted out. This ensures that the implementation of the opt-out mechanism is documented and subject to public scrutiny.

5.5.1.2 National discretion

In addition to their legal duties, HDABs may take on supportive roles to enhance awareness and understanding among citizens. While these actions are not mandated by the regulation, they are recommended good practices:

- **Public outreach and awareness**
  HDABs may engage in campaigns to raise awareness about the right to opt out. This could involve developing educational materials, partnerships with civil society groups, or providing public information sessions.
- **Guidance and interpretation**
  HDABs may provide neutral, plain-language explanations about the implications of opting out, including how it affects the availability of data for research, public policy, and innovation.
- **User support services**
  HDABs could establish multichannel support systems, such as helplines, online chats or physical service points to guide citizens through the opt-out process. Multilingual and accessible formats would help reach diverse user groups, including those with limited digital literacy.

Still, Article 84 (1) of the EHDS Regulation provides “Member States shall promote and support digital health literacy and the development of relevant competences and skills for patients. The Commission shall support Member States in this regard. Awareness-raising campaigns or programmes shall aim, in particular, to inform patients and the public at large about primary use and secondary use in the framework of the EHDS, including the rights arising from it, as well as the advantages, risks and potential gains for science and society of primary use and secondary use.”

5.5.2 Information to be communicated to citizens regarding the right to opt out

5.5.2.1 Legal Requirements by the Regulation

HDABs or other competent national authorities, are responsible for ensuring that individuals are fully informed about the opt out right through clear, accessible, and proactive communication.

Minimum required information

1. **Existence and nature of the right**

Citizens must be informed that they can opt out of the secondary use of their personal electronic health data. This applies to data used for research, public policy, innovation, and similar purposes.

2. **Voluntary and reversible nature**
   The opt-out is voluntary. It can be exercised at any time and reversed without needing to provide a justification.
3. **Scope of the opt-out**
   The opt-out applies to any secondary use processing based on data permits or health data requests approved after the opt-out is registered, as per Article 71(3). It does not apply retroactively to processing authorised before the opt-out was exercised.
4. **How to exercise the right**
   Clear, step-by-step information should be provided on how to opt out. The process should be simple and usable by all individuals, including those with disabilities or limited digital literacy.

5.5.2.2 Recommended good practice

Possible communication channels include:

- Online channels - official websites, personal digital health accounts, e-health portals.
- Channels at point of care - printed materials made available at hospitals and clinics, digital information kiosks in healthcare facilities.
- Official health insurance websites.
- Mass media channels - public service messaging, official social media accounts.
- Direct interaction with individuals - information hotlines, in person assistance at local authority offices.
- Stakeholder engagement - engagement with patient organisations and healthcare professional networks; development of information materials for distribution through these channels.

Impact of the opt-out

Citizens must be told that opting out means their data will not be used pursuant to future secondary use applications that involve identifiable information. However, opting out does not stop their data from being stored or used for delivering healthcare, nor does it prevent reporting obligations under public health law.

Identity and contact of the HDAB

Citizens must be informed which authority is responsible for managing opt-out declarations. Contact details, including email, website, and service hours, should be published.

Transparency and visibility of data use

Citizens should know that public registers exist where they can see who has received data permits, for what purpose, and under what legal basis. They should also be able to access information about whether their opt-out has been respected. The existence and purpose of opt-out registries must also be communicated clearly to individuals, e.g., in the contact channels for declaring the opt-out.

Where Member State law provides for a mechanism to implement an exception from the right to opt out [referred to in Article 71(4)], information about this should be included in the HDAB’s

information duties. The information provided should include explanations of the structure of the mechanism, how decisions to make opted-out data available are made and information about applications that have been granted/refused in respect of this exception. Further, where national opt-out implementation includes both an exception and a granular opt-out, clear and understandable explanations should be provided on the difference between these elements, how they operate separately and cumulatively.

General public awareness

Member States are responsible for ensuring that the population is broadly aware of the opt out right. This can include collaboration with patient associations, educational campaigns, or integration into digital health literacy programs

5.6 Data use before opt-out

The following chapters address data processing in three scenarios: (1) before individuals exercise their right to opt out, (2) after they have opted out, and (3) after a previous opt out has been revoked.

The following description applies equally to natural persons who do not opt out at all or who have not opted out until a given point in time but will exercise this right in the future.

In respect of natural persons who do not exercise or have not yet exercised their right to opt out, personal electronic health data relating to such natural persons shall be made available or otherwise processed (pragmatically means to cover all secondary use processing) based on data permits issued pursuant to Article 68 or health data requests pursuant to Article 69 of the EHDS Regulation.

According to Article 58 (1)(f) of the EHDS Regulation, HDABs shall make information on the conditions under which electronic health data are made available for secondary use publicly available, easily searchable through electronic means and accessible for natural persons, which information shall cover “who has been granted access to datasets of electronic health data and to which datasets they were granted access and details of the data permit regarding the purposes for processing such data as referred to in Article 53(1)”.

5.7 Data use after opt-out

5.7.1 Legal Requirements by the Regulation

The opt-out prohibits the processing of identifiable personal electronic health data under any new permits/requests approved after opt-out declaration

Temporal effect: the exercise of the right of opt-out by natural persons shall not affect the processing for secondary use of personal electronic health data relating to those natural persons pursuant to data permits or health data requests that were issued or approved before the natural persons exercised their right to opt out. In other words, the right to opt out does not have a retrospective effect: it only applies to processing operations approved after the opt-out has been exercised [Article 71(3)]. The opt-out applies to new permits and decisions issued after the decision to opt out has been registered. The list of people who have opted out is not static; it changes each day as new decisions to opt-out or to reverse opt-outs are made. For this reason, HDABs will have to consider deploying technical systems to record opt-out decisions with sufficient functionality to retrieve the list of opted out persons as it existed the date a particular permit issued. Reversing an opt-out decision should act in the same way. A person’s data may be processed in respect of permits and decisions issued after they reverse the opt-out decision.

It means, if the data of a natural person are made available pursuant to a permit issued and this person opts out on a day later than the day of issue of the permit, the content of the Secure Processing Environment (SPE) will not change. Without this rule, which was made for policy/scientific reasons, and with a retroactive opt out right, the scientific integrity of results would be jeopardised, and it would be impossible to check the correctness of analyses.

5.7.2 National discretion

It is important to add that using the opt-out from secondary use under the EHDS does not affect other reporting obligations, e.g. for health professionals.

According to Article 71 (4) of EHDS Regulation - having regard to Recital 54 - Member States may, under certain purposes with a strong link to the public interest (e.g., significant health threats), provide exception from opt-out based on national law. However, the EHDS Regulation does not automatically allow Member States to bypass opt-out decisions. They may only do so under the strict conditions of Article 71(4), which must be defined in national law, justified by important public interest, limited to public bodies / tasks and proportionate and with strong safeguards. If the Member States’ legal conditions established within the framework of Article 71(4) are met, then such data of a natural person who opted out can be processed pursuant to data permits and decisions. This exception applies only to personal electronic health data held in a dataset accessible in or falling under the legislation of that Member State. It is therefore important to emphasize about the conditions of expression, that the Article 71 (4) (a-c) state, it must involve a public institution, be necessary for listed purposes, not obtainable otherwise, and include appropriate safeguards. must involve a public institution, be necessary for listed purposes, not obtainable otherwise, and include appropriate safeguards.

5.8 Data use after the revocation of opt-out

The exercise of the opt-out right is reversible meaning that natural persons can reverse their opt-out decision any time and without providing any reason or justification.

The reversal takes effect for data permits and health data requests approved after the reversal has been registered. From that day on, the personal electronic health data of the natural person accessible and identifiable in a dataset can be included into new processing activities, provided that all other conditions under the EHDS Regulation are met. In practice, it will apply to future data permits and decisions including ongoing data access applications and data requests under assessment.

5.9 Reaction to opt-out?

5.9.1.1 National discretion

If designated by the Member State, the HDAB may also act as a contact point, though this presupposes a role in managing opt-out decisions.

Any use of opt out registry data for purposes beyond its original function, such as profiling, targeted outreach, or analytics, would risk breaching key GDPR principles, including purpose limitation [Article 5(1)(b)] and data minimisation [Article 5(1)(c)], and would therefore not be compatible with the EHDS. Under the EHDS Regulation, the opt out mechanism is intended to ensure meaningful control over secondary use and repurposing this data for re-engagement would contravene that intent unless explicitly authorised by law and supported by an appropriate legal basis.

Responses to opt-out declarations must be lawful, minimal, and strictly in service of the individual’s rights – not institutional convenience or persuasion. The aim must be to uphold informational self-determination without overburdening or alienating the data subject.

6 Annexes

6.1 Annex I – Glossary

TERM	DEFINITION
Anonymisation	The process by which personal data is altered in such a way that a data subject can no longer be identified directly or indirectly. (Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, Recital 52; EHDS Regulation, Recital 92)
Benefit (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))
Data access	Processing by a data user of data that has been provided by a data holder, in accordance with specific technical, legal, or organisational requirements, without necessarily implying the transmission or downloading of such data. (DGA, Article 2(8)(9)(13))
Data controller	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 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

TERM	DEFINITION
	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 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 & 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))
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

TERM	DEFINITION
	available datasets and their characteristics (EHDS Article (77(1))
Electronic health data	Personal or non-personal electronic health data (EHDS Article 2(2c)).
EU dataset catalogue	A dataset catalogue means a collection of dataset descriptions, arranged in a systematic manner and including a user-oriented public part, in which information concerning individual dataset parameters is accessible by electronic means through an online portal. (EHDS Regulation, Article 2(2y)) The EU dataset catalogue, the national dataset catalogues and the dataset catalogues of authorised participants in HealthData@EU shall be made publicly available. (EHDS Regulation, Article 79(1–2))
Health data access application	An application seeking to access personal-level electronic health data for secondary use in an anonymised or a pseudonymised format (EHDS Article 67).
Health data access body (HDAB)	Member state-designated authority that facilitates the secondary use of electronic health data. HDABs assess the information provided by the health data applicant and 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 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

TERM	DEFINITION
	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))
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))
Legal basis of data processing	The conditions under which personal data processing is considered lawful (GDPR, Article 6). Purposes for which the electronic health data can be processed for secondary use are laid down in EHDS Regulation, Article 53.
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 dataset catalogue	Making public, through electronic means: (i) a national dataset catalogue that includes details about the source and nature of electronic health data, in accordance with Articles 77, 78 and 80, and the conditions for making electronic health data available; (EHDS Article 57(1)(j)(i)).

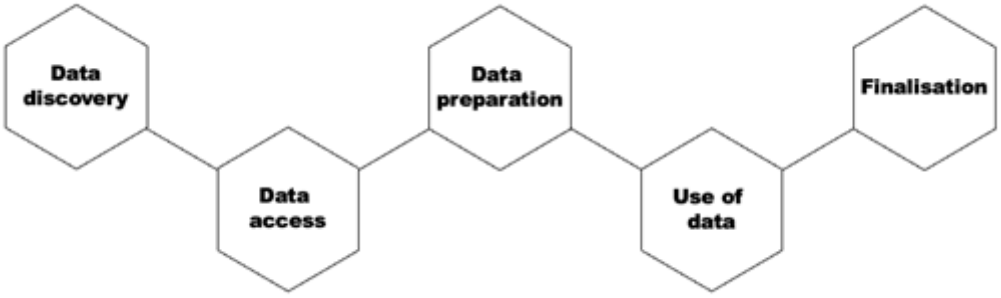
TERM	DEFINITION
National contact point (NPC)	A National Contact Point for secondary use is the organisational and technical gateway for making electronic health data available for secondary purposes, including research, innovation, policy-making, and public health. It plays a crucial role in connecting national data infrastructures to the HealthData@EU Central Platform, enabling secure and efficient data sharing across borders. (EHDS Regulation, Article 75(1))
Non-personal electronic health data	Electronic health data other than personal electronic health data, including both data that have been anonymised so that they no longer relate to an identified or identifiable natural person (the ‘data subject’) and data that have never related to a data subject. (EHDS Regulation, Article 2(2b))
Opt-out	Article 71 (1) EHDS Regulation states: “Natural persons shall have the right to opt out at any time, and without providing any reason, from the processing of personal electronic health data relating to them for secondary use under this Regulation. The exercise of that right shall be reversible.”
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))
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 organisational measures to ensure non-attribution to an identified or identifiable person. (GDPR, Article 4(5))
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.
Re-identification risk	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).

TERM	DEFINITION
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)
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 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 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)
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.

6.2 Annex II – EHDS User Journey

When a data user[i] applies for electronic health data for secondary use purposes, such as research and innovation activities, education, and policy-making, within the 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://data.europa.eu/mqa/catalogues. Once the data discovery is completed, the user can begin the process of applying for the data.

Data access

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

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

Data preparation

During this phase, the data holder(s)[iii] deliver(s) the necessary data to the HDAB, which starts to prepare the data for secondary use. Techniques for pseudonymisation, anonymisation, generalisation, suppression, and randomisation of personal data are employed. The data minimisation principle (as per the GDPR) must be respected to ensure privacy.

Use of data

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

Finalisation

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

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

[ii] 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

[iii] 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)).

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