TEHDAS2

Summary page:
TEHDAS2 public consultation on draft guideline for Health Data Access Bodies on implementing opt-out from the secondary use of health data

This consultation has 4 pages and 24 questions. The first and the second pages are common to all TEHDAS2 public consultations and cover demography of the responder and overall quality of the document. Pages 3 and 4 consist of questions specific to this document.

Demography

1. Country *

Other

2. Type of responder *

Academic or research organisation

3. Are you responding on behalf of several organisations? *

If yes: On behalf of how many organisations?

No

4. Sector *

Other
Academic Medical Center

5. Organisation size *

Small to medium enterprise (10–249 employees)

6. Professional role / function

Academic research and policy center

Quality

7. Is the document easy to understand? *

3

8. How well does the document address the key issues related to its subject matter? *

3

9. How feasible do you find the guidelines or technical specifications to implement, as outlined in the document? *

2

10. Generic feedback

Do you have any suggestions for improving the document? Are there any additional topics or areas that should be covered? Max. 5000 characters.

The aspirational goals of the EHDS are commendable: to make health data accessible for research, innovation, and evidence-driven policymaking. To effectuate these goals, representative datasets must be available at scale, balanced by protections to the individual, ensuring privacy and autonomy. The ability to opt out in a way that is or should be simple, reversible, and without requiring justification or a reason is intended to provide a means of exercising individual choice.
The challenge, however, is that the EHDS and its implementing guideline M8.1 allow such flexibility, differences in opt-out systems, and variations in implementation practices that the real risk of dataset fragmentation exists, undermining its usability and the very reason for creating the EHDS. While appreciating the goal of empowering Member States to develop their own opt-out approaches, common definitions, data structures, metadata, and other factors must be coordinated and agreed upon to ensure interoperability and usability. The power of the EHDS rests, at least in part, in its scale and representativeness: the proposed optionality will result in data fragmentation and limit this power. There must be a consensus on core definitions and functionalities (e.g., methods of anonymization or pseudonymization) for the EHDS effort to deliver on its promise and justify the expense and effort.
For example, if Member States can create country-specific, granular opt-out categories (e.g., opting out of genomic data in one state, EHR data in another, and research in a third), it may be impossible to develop a combined dataset that is representative of the populations of the Member States. The same challenges exist if the methods of anonymizing one set of data differ from another.

In general terms, the plan for cooperative (if not unified) governance is unclear, as is the plan for further universal implementation requirements.

It is not clear whether the legal framework is intended to apply to data "generated and held" by the Member State. ("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.") If data is not "generated" but only "held" in the Member State, what, if any, opt-out provisions apply? Does "moving the data" obfuscate the ability to opt out?

A few additional general comments on opt-out:
- Is there an appeal process for the override of an opt-out decision? Will the individual be informed?
- The DHAB is required to make available the projects that it approves but only reports on those projects that it disapproves every two years. It seems that there should also be transparency about projects that are not approved in real-time. Is there an appeal process for disapprovals?
- It is often difficult to define the purpose of AI applications with specificity. Will DHABs permit applications for injection in AI engines?
- Has there been any consideration of the costs and burdens of opt-out procedures?
- In clinical trials and in some other contexts, informed consent documents often include consideration of and permission for future data use (and, for instance, deposition in a data repository). How will the right to "opt out" via EHDS be reconciled with informed consent processes?
- How will the representativeness of the dataset be validated given the variability of opt out?

The following questions are specific for TEHDAS2 draft guideline for Health Data Access Bodies on implementing opt-out from the secondary use of health data

11. Will this guideline impact your organisation or activities?

If no: Please explain

No
We are not planning to be a HDAB

12. Is scope and aim of the guideline clearly described in the Introduction?

If no: Please explain

Yes

13. Do you find the description of the opt-out with regard to electronic health data (Chapter 2 Opt-out from what?) sufficiently clear?

If no: Please explain

Yes

14. Do you find it clear which roles with regard to the opt-out may be delivered by HDABs, data holders, trusted data holders and Member States?

If no: Please explain

No
The guideline appears to permit great variability in which entity or entities are responsible for the roles. The guideline appears to envision that the HDAB operates within a single Member State, rather than across multiple Member States. However, that may or may not be optimal or the most practical approach. The guideline explains that Member States decide implementation and may assign HDABs operational roles (registry, portal, info duties). It also notes that data holders may act as contact points and are responsible for filtering datasets at source; HDABs have reporting and information obligations if assigned the opt-out role. The clarity of roles breaks down based on both the site of data acquisition and the jurisdiction of the HDAB. A remaining ambiguity is who will perform day-to-day enforcement (HDAB vs. data holder) during data extraction for a specific permit. Will data holders (e.g., hospital systems or in the case of clinical trials, pharmaceutical sponsors) be responsible for tagging opt-out, will HDABs block at the permit level, or are other scenarios envisioned? The guideline suggests filtering options at the dataset, data holder, or HDAB level, while leaving implementation variability across Member States. A final concern is that if roles regarding opt-out can be assigned and delivered by various entities, as the guideline appears to allow, how can someone—as an individual—know who is responsible and for what?

15. Are the responsibilities of HDABs described in Chapters 3 & 4 appropriate to support the implementation of the opt-out?

If no: Please explain

No
The guideline outlines an example for processing the opt-out in which HDAB's duties include public information, maintaining searchable permit registers, publishing biennial reports, and hosting opt-out registries and portals. But again, these and other responsibilities vary depending on Member State assignment. Furthermore, there are no operational HDAB duties regarding datasets for clinical research, such as communicating opt-out changes to data holders, establishing industry standards for real-time filtering, and notifying current permit applicants or holders when opt-out rates materially affect a dataset.

16. Is sufficient detail provided in Chapter 4 "How to declare opt-out?"?

Unclear – please explain
The guideline lists acceptable channels (online portal, EHR portal, in-person) and high-level registry design principles (minimization, authentication, logging) at the conceptual level. It leaves the determination of the required technical standards (e.g., patient identifier format, dataset synchronization frequency, message formats, and how opt-out flags propagate to Secure Processing Environments) to be determined through Member State-level implementation.

17. Do you see any legal challenges in implementing the opt-out as described in the guideline?

Max. 5000 characters.

There is a risk in fragmentation and the variance of national laws.
Article 71delegates implementation to Member States. Different choices regarding the opt-out registry location (HDABs or another entity), the granularity of opt-out levels, and Article 71(4) exceptions could lead to cross-border divergence. For multinational purposes (e.g., trials and RWE datasets), the legal regimes for data availability are inconsistent.
Exceptions to opt-out ("public interest", public health emergencies, policy-making, some research, etc.): The legal basis for the permitted use of opt-out data is unclear and appears to be based on decisions made by the Member States, exposing the DHAB, data users, and others to risk. For example, if Member States enact different national exceptions or definitions of permitted uses (e.g., ("public interest", emergencies, research, policy, etc.), data users may face varying laws and processes for accessing data that have been opted out, which complicates ethics approvals and contractual terms.
Interaction with GDPR and right to object: The guideline explains that EHDS opt-out is separate from and builds upon GDPR objection/consent rights. However, translating these two parallel frameworks is complex and may need further guidance. For instance, how does consent for future use of data (and data deposited into repositories) under GDPR relate to and intersect with opt-out in EHDS?
A fundamental legal issue is that the boundary between "anonymised" (outside the jurisdiction of GDPR) and "pseudonymised but potentially re-identifiable" (subject to GDPR) data is unclear — and this matters for accessing data under secondary use and the interplay with EHDS.
Given the varying responsibilities for DHABs, data holders, and data users, and the varying decisions made by Member States, compliance will be difficult and expose these entities to legal risk.
Please see responses to question 18 as well.

18. Do you see any data protection challenges in implementing the opt-out as described in the guideline?

Max. 5000 characters.

Several data-protection–specific challenges have been identified with implementing the EHDS opt-out as described in the M8.1 Draft Guideline. Some of these overlap with general legal concerns and arise from tensions between EHDS requirements and the GDPR's strict rules on processing health data.
The EHDS allows secondary use of personal electronic health data unless a person opts out.
But GDPR requires a lawful basis for processing, plus a separate condition for processing special-category data like health data. There is no single EU-wide legal basis for secondary use under EHDS.
Member States interpret the legal bases of "public interest" and "scientific research" differently. An opt-out under EHDS does not constitute consent under GDPR, so processors must rely on an alternative legal basis.
The EHDS guideline requires that people be able to opt out at any time and later reverse their opt-out decision. Pseudonymized data are still considered personal data under GDPR. If pseudonymized data have already been shared with a data user or aggregated, the right to withdraw permission under GDPR cannot be fully operationalized.
The EHDS guideline assumes that data holders (and or the entity responsible for tracking opt-out) will reliably track opt-out decisions, communicate those decisions to HDABs and research environments, and enforce them in all processing pipelines.
Processing personal data (e.g., pseudonymized data) without respecting an opt-out (e.g., a valid objection) is unlawful. Data holders, HDABs, and research environments do not have
GDPR obliges data controllers to provide individuals with clear information about the purposes of processing, their rights, the recipients of the data, and retention periods.
Under EHDS and secondary use, there is no individual notification to data subjects when each new reuse is approved; the HDAB decisions are posted publicly, not communicated individually; and there is no responsibility to ascertain whether people understand how their data are being used.
Registry privacy risk: Maintaining a centralized opt-out registry is necessary for enforcing opt-out, but it requires a careful balance of sensitive choices regarding patients' privacy. The guideline recommends minimization, encryption, and restricted access. Member States must implement strong technical and governance safeguards to prevent misuse (profiling, recontact, inference), as breaches could damage public trust and research participation.
Anonymization/pseudonymization workflows: Because opt-out blocks processing steps that transform identifiable data into research datasets, data controllers who normally pseudonymize/anonymize datasets must adjust pipelines, ensuring that no processing happens for opted-out individuals.
Real-time synchronization of data use from multiple data holders: ensuring consistent enforcement of opt-out across all sources (and proving that enforcement for audit/inspection) requires robust provenance tracking. The guideline suggests technical integration but leaves implementation choices open.
Authentication and reversal security: Reversible opt-out requires identity verification for both declaration and reversal. For trial populations (some with limited capacity), verifying identity without over-collecting data may be challenging. The guideline notes eiDAS/national IDs as options, but uniform availability and accessibility issues remain.
Purpose limitation vs. legitimate public interest: If Member States apply Article 71(4) exceptions for public health research, controllers must implement tight safeguards (SPEs, prohibition of re-identification). Verifying that these safeguards are sufficient and enforced is technically and administratively demanding.

19. Does the guideline accurately describe the flexibility available for national implementation of the opt-out?

If no: Please explain

Yes

20. Is the level of legal and technical interoperability foreseen for national implementation sufficient to ensure harmonised implementation of the EHDS Regulation?

If no: Please explain

No
The guideline emphasizes the need for interoperable technical standards and national integration with EHDS infrastructure (e.g., tagging in EHRs, opt-out registry connections), but fails to appreciate how the permitted flexibility will result in data fragmentation that undermines harmonization and utility. It falls short of providing concrete standards (identifier format, message semantics, synchronization frequency, and error handling) that sponsors and investigators may need for cross-border studies. Without EU-level technical specs, Member State variability will remain, impairing harmonized multi-country research.

21. Is the relationship between GDPR and the EHDS Regulation regarding the opt-out clearly explained (Introduction and Chapters 1, 2, & 9)?

If no: Please explain

No
The guideline clearly states that the EHDS opt-out is a specific right and complements the GDPR. While it explains the differences between consent and the GDPR right to object, it fails to clarify or reconcile the many differences between the two. Please see responses to questions 17, 18, and others for further comments.

22. Are the recommendations for engagement and empowerment appropriate to support implementation of the right to opt?

If no: Please explain

No
The guideline's emphasis on transparency, citizen engagement, tailored literacy programs, and stakeholder forums is appropriate and important to avoid opt-out-driven bias. The guideline does not clarify how the diversity of stakeholders will be represented, assessed, and/or engaged. This is of particular concern with respect to underserved and minoritized populations, those less familiar or comfortable with digital technologies, those unfamiliar with health-data governance, the elderly, and others. Availability of the information on opt out is not the same as accessibility or proactive engagement. The EHDS guidance does not mandate minimum outreach, periodic reminders, or targeted campaigns, and is thus likely insufficient for equitable empowerment. How engagement will be funded, operationalized, and sustained remains unclear. There is no expectation that periodic assessment or metrics for engagement and/or empowerment will be performed, leaving open the possibility that implementation will be uneven. Sponsors and investigators may benefit from HDABs producing trial-specific communications (explaining how opt-out interacts with trial consent, data used in trials, safety reporting, and follow-up). The guideline recommends engagement but doesn't require EMA/ethics-level materials for trial settings.

23. Are the proposed steps for implementing the right to opt-out feasible for HDABs to adopt in practice?

If no: Please explain

No
Feasibility depends on technical capacity, funding, and clear assignment of responsibilities. The steps (creating registries; designing portals; informing the public; coordinating with data holders; building filtering at the source or dataset level) are technically feasible but will require significant investment, standardized technicalities, and governance arrangements. Smaller Member States or data holders may face capacity constraints, and staggered implementation may create temporary operational barriers for clinical research.

24. Which sections or subject matter in the document require further elaboration?

Max. 5000 characters.

Key areas that may benefit from expanded guidance:
Additional clarification would be appreciated on technical interoperability specifications, standards for opt-out processing, state-level governance on mandated timelines for registry updates, notification obligations to data holders, and audit rights for sponsors to verify that opted-out patients were excluded from datasets used in trials. Clarity on liability in case of accidental inclusion should be provided.
More detail on national Article 71(4) exception processes for harmonized implementation of opt-out across EU (justification thresholds, oversight and safeguards) would be beneficial.
Authentication & capacity handling: guidance on identity verification processes for patients with limited capacity and on how parental/guardian opt-outs interact with later attainment of legal capacity are insufficiently explored.
End-to-end worked examples for clinical research flows (EHR → data holder extraction → pseudonymisation → SPE → permitted research), including decision points when opt-out must be checked, including multicenter and cross-border scenarios and, specifically, the application to clinical trials and clinical research. Data to support regulatory review of medicinal products depends on completeness and the ability to audit; opt-out is problematic in this setting.
Further guidance for clinical trials and the interplay with informed consent: specific guidance clarifying how EHDS opt-out interacts with trial consent (e.g., does trial consent override opt-out for trial data? Does trial use remain the primary use and/or rely on different provisions?) The guideline should clarify practical steps when trial participants opt out. Plain-language scripts for investigators to explain consequences to participants.

Finish