DIGITALEUROPE

15 January 2026

Safeguarding intellectual property and trade secrets in the European Health Data Space

Executive summary

The objective of the European Health Data Space (EHDS) of enabling the responsible re-use of health data for research, innovation, and public health requires a governance framework that protects intellectual property (IP), trade secrets and commercially confidential information, which Europe's capacity to innovate depends on.[1]

The EHDS represents an unparalleled opportunity to advance research, innovation and patient care. Yet its success will depend on achieving the right balance between open data access and the protection of confidential information that drives innovation.

The EHDS introduces obligations that could bring privately held or pre-commercial data into scope for secondary use.[2] Their implementation must strike a careful balance between openness and the protection of legitimate proprietary interests. The EHDS will only succeed if innovators, researchers and manufacturers can participate in data-sharing mechanisms without risking the loss of valuable know-how or competitive advantage.

With no implementing act attached to Art. 52 (IP and trade secrets), the risk of fragmentation is high, and implementation guidelines are needed to ensure a workable and harmonised EHDS framework that supports innovation.

These implementation guidelines should:

- Encourage Member States to establish **dedicated IP and trade secret task forces within health data access bodies (HDABs)**, equipped with the legal, technical and industrial expertise needed to assess data requests involving commercially confidential information;
- **Allow health data holders to indicate the confidentiality level and access conditions for each dataset and its metadata**, so that sensitive information is not inadvertently exposed through the EHDS catalogues;

[1] Regulation (EU) 2025/327.

[2] Art. 52 EHDS requires that electronic health data protected by IP, trade secrets and regulatory data protection be made available 'in accordance with this Regulation,' but it also allows HDABs to refuse access when disclosure would entail a serious risk of infringement (Art. 52(5)).

DIGITALEUROPE
Rue de la Science, 37, B-1040 Brussels
+32 2 609 53 10 ▶ Info@digitaleurope.org
▶ www.digitaleurope.org
EU Transparency Register: 64270747023-20

- **Outline best practices around existing legal, organisational and technical safeguards**, including contractual terms, confidentiality clauses, secure processing environments and proportionate technical controls developed in consultation with health data holders and other relevant entities;
- **Ensure structured cooperation between HDABs, health data holders and rights holders**, so that those who understand a dataset's sensitivity are actively involved throughout the access and permitting process;
- **Further delineate the scope of the categories of data in Art. 51** to avoid excessive disclosure obligations on health data holders, particularly in the case of early-stage R&D and raw medical-device data. The guidelines should require HDABs to consult data holders and rights holders before deciding whether data can be shared.[3]
- **Clarify the complaint and liability mechanisms**, including suspension of data use whilst a permit is under review and transparent allocation of responsibility for misuse or data breaches.

Investing resources in harmonised guidance on the key elements outlined above will be decisive for the overall success of this landmark law. A coherent and well-resourced approach will ensure that the EHDS becomes a trusted and harmonised framework, enabling data-driven research and innovation whilst preserving the incentives that make such innovation possible.

DIGITALEUROPE stands ready to work closely with the European Commission, Member States and the HDAB Community of Practice to ensure that EHDS implementation strengthens Europe's global leadership in healthcare.

This paper is endorsed by key industry partners who share DIGITALEUROPE's vision for a fair and workable European Health Data Space that protects innovation while enabling secondary use of health data.

COCIR Advancing Healthcare

efpia

EUCOPE European Confederation of Pharmaceutical Entrepreneurs AISBL

MedTech Europe from diagnosis to cure

[3] The EHDS implementation guidelines could build on the approach taken in the recent *Guidance on vehicle data, accompanying the Data Act* (C(2025) 6119 final), which explains how key obligations apply to vehicle data and sets out sector-specific access rules for original equipment manufacturers, suppliers, aftermarket service providers and insurers.

Table of contents

Establishing dedicated IP and trade secret task forces within HDABs

Health data access bodies (HDABs) will play a central role in ensuring consistent interpretation of Art. 52 EHDS across Member States. Their credibility will depend on their ability to handle commercially confidential information with confidence and to gain the trust of health data holders and innovators.

Art. 57(c) tasks HDABs with balancing the rights and interests of both health data holders and health data users. This role includes taking appropriate legal, organisational and technical measures to protect IP, trade secrets and regulatory data protection, as required by Art. 52. HDABs' competence and resources will therefore directly determine whether the EHDS can achieve its objectives without undermining innovation incentives.

Member States are currently defining their HDABs' structures, mandates and resource allocations, supported by initiatives such as TEHDAS2,[4] the HDAB Community of Practice and, more recently, the Innovative Health Initiative project 'Safeguarding innovation in secondary use of health data in the European Health Data Space.'[5] Whilst several Member States already operate frameworks for secondary data use, the EHDS significantly expands the scope of data and actors involved. For the first time, private health data holders will be required by 2029 to describe their datasets in the EU-wide catalogue and respond to data-access requests, which demands that HDABs develop the expertise and safeguards needed to handle commercially confidential information effectively.

DIGITALEUROPE calls on Member States to **establish specialised task forces within HDABs focused on requests that involve innovation, IP, trade secrets, regulatory data protection or other commercially confidential information**. These task forces should include staff with the necessary technical, legal and industrial expertise to assess and issue data permits involving such data. Many existing HDABs already handle secondary use of public-sector data, but have limited experience with privately held or mixed datasets. Building this capacity is essential to ensure consistent, predictable and harmonious decisions across the Union.

Close **cooperation between these national task forces** is equally important. They should operate as an operational bridge between Member States and EU-level coordination structures, translating the work of the HDAB Community of Practice and, in due course, the EHDS Board into national procedures. Industry representatives and **rights-holder organisations should be systematically involved to ensure that evolving practices reflect technological realities and market dynamics.**[6]

---

[4] https://tehdas.eu/.

[5] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-ju-ihi-2025-10-02-two-stage.

[6] The TEHDAS2 *Draft Guideline for Health Data Access Bodies on minimum categories and limitations on the reuse of health data* similarly calls for structured exchanges between HDABs and health data holders. It recommends that HDABs identify practical examples of legal, organisational and technical protective measures for IP and trade secrets; develop a best-practice list to promote uniform assessments across Member States; and establish a checklist of actions for handling IP and trade secrets. See TEHDAS2 *Guideline 5.2*, available at https://tehdas.eu/public-consultations/. See also the 'Collaboration between HDABs, health data holders and rights holders' section below.

At the EU level, the HDAB Community of Practice should create a **permanent working group on innovation and IP protection**, operating transparently and in collaboration with industry, academia and research organisations. The European Union Intellectual Property Office and the European Patent Office should also be associated with this work, contributing their expertise and helping to disseminate IP best practices across the network. Once the EHDS Board becomes operational in 2027, the findings and recommendations of this working group should be integrated into its agenda to ensure that IP protection remains a central feature of the EHDS governance framework.

Finally, the Art. 72 procedure for designating 'trusted health data holders' should be implemented uniformly and transparently across the EU. The process must be simple and non-burdensome, enabling swift certification and efficient oversight of sensitive data flows.

Enabling health data holders to indicate confidentiality levels and access conditions

Protecting health data holders' IP and trade secrets requires an EHDS technical architecture and governance processes that enable health data holders to specify, with appropriate granularity, the level of confidentiality associated with each dataset and corresponding metadata. This is essential to prevent inadvertent disclosure of proprietary methodologies, data structures or commercially confidential insights.

Within most organisations, datasets are already classified internally according to a tiered confidentiality model that governs sharing within and outside the company. The EHDS should build on these established practices by allowing health data holders to communicate confidentiality levels to the relevant HDAB when submitting dataset descriptions and by ensuring that those classifications meaningfully shape the assessment of data access applications.

Building on the findings of the EHDS2 Pilot Project and the TEHDAS2 Joint Action, the HealthDCAT-AP standard has been identified as the common metadata model for dataset descriptions.[7] To respect health data holders' rights under Union law, this standard must include attributes that allow them to indicate the confidentiality level and required safeguards for each dataset and its metadata. **HealthDCAT-AP should contain a dedicated and broad 'confidential information' property**, with subclassifications for IP, trade secrets, regulatory data protection, commercially confidential information and any other relevant rights. While some clarification was provided in the outcomes of the TEHDAS2 5.1 *Guideline for health data holder* [8] and the recent HealthDCAT-AP Release 5[9], these do not provide the level of granularity needed to allow health data holders to satisfactorily disclose the level of protection of the data nor mitigate the risk that

[7] Metadata in the context of this paper refers to what is mandated in Art. 77(1) of the EHDS Regulation: '*Health data access bodies shall, through a publicly available and standardised machine-readable dataset catalogue, **provide a description in the form of metadata of the available datasets and their characteristics**. The description of each dataset shall include information concerning the source, scope, main characteristics, and nature of the electronic health data in the dataset and the conditions for making those data available.'*

[8] See TEDHAS2 results guidelines 5.1, section 9.3, July 2025, available at https://tehdas.eu/results/

[9] https://healthdataeu.pages.code.europa.eu/healthdcat-ap/releases/release-5/.

metadata and dataset descriptions may themselves reveal confidential information, for example, by exposing the scope of a company's research focus or the structure of a proprietary database.

Arts 77 and 79 EHDS mandate the creation of national and EU-level dataset catalogues through an implementing act that will specify the minimum metadata elements to be provided by data holders. These acts and associated guidelines must recognise that certain **metadata and its description in the publicly available dataset catalogue may itself require protection**. The Commission should ensure that health data holders can label the confidentiality not only of the dataset but also of its metadata before publication in public catalogues.

Art. 52(2) provides that health data holders must inform HDABs when datasets include IP or trade secrets. Similarly, this obligation should be understood as extending to both datasets and their associated metadata. HDABs should give due weight to the classification assigned by data holders and accept it as determinative unless clearly incorrect. Such recognition would reflect the principle of proportionality embedded in Art. 52 and maintain a fair balance between openness and protection of proprietary information.

When exercising this right, health data holders must also be able to identify datasets whose disclosure for specific purposes would entail a **serious risk of infringing IP, trade secrets or regulatory data protection under the Medicinal Products Directive or the Medicines Authorisation Regulation**.[10] In such cases, HDABs should treat this designation as a legitimate ground for refusing access, consistent with Art. 52(5) EHDS. **A clear procedure should be defined, through implementation guidance, allowing data holders to flag these risks and provide justifications.**

Measures to protect IP and trade secrets in databases

Art. 52(4) EHDS provides that, when issuing data permits, HDABs may make access to electronic health data conditional upon legal, organisational and technical measures. These measures may include contractual arrangements between health data holders and health data users where the data contains information protected by IP or trade secrets. The Commission is tasked with developing non-binding model contractual terms for such arrangements.

Innovators, whether research institutions, universities or companies, already rely on sophisticated contractual and technical frameworks to share data responsibly whilst preserving their IP, trade secrets and other commercially confidential information. **Implementation guidelines should build on these practices rather than reinvent them**, ensuring compatibility with existing confidentiality regimes and innovation incentives.

Legal measures

Health data holders should always have the possibility to conclude a contractual arrangement with the health data user before access is granted. Such agreements remain the most effective means of ensuring that rights and responsibilities are clearly defined. They should normally include confidentiality clauses, provisions on IP ownership and explicit terms on how any new IP arising from the permitted processing will be allocated or licensed.

[10] Art. 10(1) Directive 2001/83/EC and Art. 14(11) Regulation (EC) No 726/2004, respectively.

Depending on the sensitivity of the dataset, the health data holder may retain ownership of any resulting IP or grant a limited, non-exclusive licence to the data user (or vice-versa). The contract may make it clear that data accessed under a permit cannot be used to develop a competing product or service, reflecting Art. 11(2)(b) Data Act. Where the applicant operates in the same sector as the health data holder, or the research could generate commercially exploitable results, access should be subject to stricter justification and additional safeguards.

Publication of research results must also respect these protections. Although Art. 61(4) EHDS requires health data users to publish results within eighteen months of completing their processing, justified exceptions exist. Where the data concerns IP, trade secrets or regulatory data under the Medicinal Products Directive or the Medicines Authorisation Regulation, publication may need to be delayed, redacted or, in exceptional cases, withheld altogether. In such instances, publication rights and timing should be defined by agreement between the health data holder and the health data user.

Finally, contractual arrangements must contain **enforceable remedies** – injunctive relief, compensation and termination of access – so that breaches of confidentiality or misuse of data can be addressed effectively.

Organisational measures

In addition to contractual tools, HDABs must establish robust organisational safeguards to prevent unauthorised access and ensure that data identified as sensitive is handled only by qualified personnel. **Dedicated departments within HDABs should process data access requests made for development and innovation activities for products or services**.[11] These departments should include staff trained in IP and data protection law. **All personnel engaged in such decisions should be bound by non-disclosure obligations and clear internal confidentiality policies.**

HDABs should carry out risk assessments for datasets flagged as containing IP, trade secrets or commercially confidential information. These assessments should be conducted in cooperation with the health data holder and, where applicable, the rights holder, in line with Art. 57(1) (c) EHDS, which requires HDABs to take all measures necessary to preserve confidentiality. Before a permit is issued, the HDAB should verify with the health data holder that the proposed safeguards correspond to the dataset's sensitivity.

Where commercially confidential information is involved, **the health data holder, or the IP or trade-secret holder if different, should have the right to review research outputs prior to publication**. This review should focus on whether the results reveal proprietary annotations or datasets still protected by exclusivity.

Technical measures

Technical safeguards must operationalise the protection of trade secrets and IP throughout the data access process. Whilst the EHDS already mandates **secure processing environments, anonymisation and pseudonymisation**, these requirements must be implemented in a way that anticipates real-world risks.[12]

[11] Art. 53(1)(e) EHDS.

[12] Examples of relevant technical safeguards include: role-based access control; multi-factor authentication; encryption in transit, at rest and, where relevant, during processing (confidential computing); data anonymisation, pseudonymisation and masking; continuous audit logging and real-time monitoring for suspicious activity; smart-contract or rule-based enforcement of access

Data holders should remain responsible for data minimisation and redaction before transfer and should be empowered to tailor datasets to what is strictly necessary for the authorised purpose.

Secure environments must prevent the downloading of raw data and include continuous monitoring for suspicious activity. Real-time alerts should detect excessive queries, attempts to reconstruct datasets or code execution aimed at revealing embedded proprietary logic. In high-risk cases, the HDAB should work with the health data holder to ensure that the secure environment's technical configuration meets the holder's security standards.

Comprehensive audit logs should record every access and action performed on sensitive datasets to enable full traceability and accountability. Common industry techniques – role-based access control, multi-factor authentication, encryption in transit and at rest, confidential computing, data masking, smart-contract monitoring and data-loss-prevention tools – should all be available for use, with their application determined case by case in consultation with the data holder.

Collaboration between HDABs, health data holders and rights holders

Art. 52 EHDS cannot fulfil its purpose without close and continuous cooperation between HDABs and those who hold the rights to confidential data. It demands an active exchange in which those who understand the data's structure, sensitivity and commercial value can explain the implications of disclosure and the protective measures needed.

In practice, this means that **HDABs must work directly with health data holders and, where applicable, with the IP or trade secret holders, who may not be the same entity**.[13] Without such engagement, HDABs lack the information needed to assess the risk of infringement or the adequacy of safeguards. The **Commission's implementation guidelines should make this cooperation an integral part of the assessment process**, setting clear expectations for dialogue and documentation at every stage, from initial notification to the evaluation of data access applications.[14]

When notifying an HDAB that a dataset contains IP or trade secrets, the health data holder should specify the type of protection required and the safeguards that must be applied.[15] Health data holders should be

conditions; data-loss-prevention tools; and, where appropriate, limited-functionality or federated-learning environments that enable analysis without exporting raw data.

[13] For instance, in the case of data originating from medical devices, a hospital may be the health data holder, but not the owner of the embedded algorithms or calibration methods protected as trade secrets by the device manufacturer. In such situations, HDABs should systematically consult both the health data holder and the underlying rights holder to determine whether the proposed access and protective measures are appropriate.

[14] This approach is consistent with the Trade Secrets Directive (Directive (EU) 2016/943) and the WTO Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), which both affirm the right of trade secret holders to maintain control and oversight of their confidential information. It would also bring the EHDS in line with the logic of the Data Act, where the data holder and recipient must jointly agree on measures to protect trade secrets, proportionate to the nature of the data and the risk involved.

[15] As previously argued, this should cover both the dataset and its metadata, since metadata can in some cases reveal confidential business information, such as the scope of ongoing research or the structure of proprietary databases.

able to advise HDABs on the level of detail appropriate for publication in the EU and national catalogues, ensuring transparency without compromising commercial assets.

Under Art. 57(1)(c) EHDS, HDABs must take all measures necessary to preserve the confidentiality of both health data holders' and users' interests. This obligation implies an active dialogue: **before granting access, HDABs should provide health data holders with the identity of the applicant, the intended use and the protective measures proposed**. The health data holder's expertise is critical to assessing whether disclosure might lead to a competing product or whether pre-existing contractual obligations restrict sharing. Without such input, HDABs cannot meaningfully fulfil their duty to balance interests.

To reinforce uniform practice, implementation guidelines should therefore mandate structured cooperation between HDABs and health data holders in all cases involving IP, trade secrets or regulatory data protection and innovation activities. The HDAB, as the authority issuing data permits, should be required to consult the health data holder and the rights holder where applicable, document the consultation process and justify any decision that departs from their recommendations.

Categories of data for secondary use

Art. 51 EHDS obliges health data holders to make data available for secondary use when it falls within one of the listed categories. The provision is central to the functioning of the EHDS, but its breadth creates uncertainty, particularly where the listed categories may overlap with information protected by IP, trade secrets or regulatory data protection. To prevent unintended disclosure and to ensure consistent application, **the Commission should clarify, through implementation guidelines, how these categories are to be interpreted in practice**.[16] These should build on the results of the TEDHAS2 5.1 *Guideline for data holders on data description*, which provides some level of clarification around the data in the scope of each category.[17]

Many of the categories listed in Art 51 – those covering data from biobanks, registries, research cohorts, genetic and genomic data, and laboratory results – may include datasets generated during early-stage research and development.[18] Similarly, Art. 51(p) on data from research cohorts, questionnaires and surveys is drafted broadly and could capture a wide range of ongoing research activities. Such data, whilst not patentable in itself, can disclose valuable insights into ongoing scientific work, future innovation strategies and commercial pipelines, and therefore constitutes commercially confidential information. It is a

[16] The recently published FAQ document provided some clarification around certain data categories. For instance, for Art. 51(m) on 'data from clinical trials, clinical studies and clinical investigations,' it has been clarified that this should be interpreted as referring to data from completed studies, where results have already been made publicly available, and not data from ongoing trials, studies or investigations. However, for other data categories, further clarification is required. See European Commission, *Frequently asked questions on the European Health Data Space*, March 2025, available at https://health.ec.europa.eu/document/download/4dd47ec2-71dd-49fc-b036-ad7c14f6ed68_en?filename=ehealth_ehds_qa_en.pdf.

[17] TEDHAS2 5.1 guideline results provide useful clarifications on certain categories. For instance, for Art. 51 (1(h), it clearly states that 'data stored locally on devices without sharing or syncing to health data holders' is out of scope. For Art. 51 (1) (m), the guideline further confirms that ongoing trials, trials under data protection or exclusivity are out of scope. For Art. 51 (1)(n), it states that device-specific logs unrelated to health metrics are not in scope. However, Art. 51 (1) (b) (d) (f) and (g) remain broad and by their very nature could capture a vast range of data held by health data holders. See TEHDA2 result guidelines 5.1, July 2025, available at https://tehdas.eu/results/.

[18] Arts 51(b), (d), (f) and (g) EHDS.

legitimate and established practice for companies, research organisations and academic institutions to keep such data confidential until the resulting innovations are adequately protected.

Similar caution is needed for data generated by medical devices. Arts 51(h) and (n) should be read as referring only to processed, human-readable information consistent with what is accessible to the patient or healthcare provider. **Raw machine data used internally by the manufacturer to derive diagnostic scores or outcomes remains proprietary and should fall outside the scope of the EHDS**.

When preparing implementation guidelines, the Commission should provide a clearer list of data types – comparable in precision to Annex I for primary-use data – developed in close cooperation with health data holders and rights owners. The guidelines should ensure that in all these cases, HDABs actively involve health data holders and, where applicable, IP or trade-secret owners to determine whether a dataset falls within Art. 51. Clearer boundaries will safeguard R&D activities and foster trust in the EHDS framework.

Right to lodge a complaint and liability

The EHDS establishes the right for both health data holders and health data users to challenge HDABs' decisions. However, the current provisions leave important procedural and liability aspects undefined, creating uncertainty for all entities involved in the secondary use of health data. Clear rules are needed to ensure that complaints are handled effectively and that responsibility is appropriately allocated across the different stages of the data access process.

Liability should be assessed distinctly according to the phase in which an incident occurs. Three stages can be identified: the data permit and complaints phase; the data use phase; and the phase covering breaches or leaks. This delineation is necessary to ensure that each actor's responsibilities are transparent and proportionate to its role.

During the data-permit and complaints phase, Art. 52 grants both health data holders and users the right to lodge a complaint under Art. 81. Yet, Art. 81 does not specify what happens to an authorised data permit whilst a complaint is pending. To protect the interests of both data holders and data subjects, **the data sharing activity covered by the contested permit should be suspended until the HDAB has issued a formal decision** on the complaint or, where the decision is appealed, until the competent court has delivered a ruling. Such a suspension mechanism would prevent irreversible harm from premature data re-use.

In the data use phase, liability should rest primarily with the health data user whenever data is misused, misappropriated or applied for unauthorised purposes. Users must operate strictly within the parameters of their data permit, the SPE and any contractual restrictions agreed with the health data holder. Misuse of data that infringes IP, trade secrets or regulatory data protection should entail administrative penalties and potential civil liability.

In contrast, **when a breach or leak occurs within an SPE, or because of inadequate organisational safeguards, liability should be borne by the HDAB or by the service provider** operating that environment. As the entities responsible for maintaining the technical and procedural integrity of data processing, they must ensure that appropriate security, monitoring and access-control measures are in place, and that audit trails allow for accountability.

Finally**, the Commission's implementation guidelines should clarify how the complaints mechanism and liability framework interact**, setting out standard timelines for responses, the scope of remedies and coordination with national judicial systems.

FOR MORE INFORMATION, PLEASE CONTACT:

Gianluca Violante

Senior Manager for Digital Health Policy

gianluca.violante@digitaleurope.org / +32 492 46 78 17

Alberto Di Felice

Policy and Legal Counsel

alberto.difelice@digitaleurope.org / +32 471 99 34 25

About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory and investment environment that enables European businesses across multiple sectors, as well as citizens, to prosper through digital technologies. We wish Europe to grow, attract and sustain the world's best digital talent, investment and technology companies. Together with our members, we shape industry positions on all relevant policy matters and contribute to their development and implementation. Our membership represents over 45,000 businesses who operate and invest in Europe. It includes corporations and scaleups which are global leaders in their fields, as well as national trade associations from more than 30 European countries.

DIGITALEUROPE
Rue de la Science, 37, B-1040 Brussels
+32 2 609 53 10 ▶ Info@digitaleurope.org
▶ www.digitaleurope.org
EU Transparency Register: 64270747023-20