Workshop on IP Rights and Trade Secrets in Relation to the EHDS

TEHDAS2 – Second Joint Action Towards the European Health Data Space

12 March 2026

Brussels

Co-funded by the European Union

About the workshop

The workshop on intellectual property (IP) rights and trade secrets aimed to clarify stakeholder needs and concerns related to IP, trade secrets, and regulatory data protection in the context of secondary use under the European Health Data Space (EHDS). Bringing together 75 participants on-site and more than 150 online, including health data holders from both industry and academia, health data access bodies (HDABs), and health data users, the workshop sought to build a shared understanding of key challenges across the secondary use workflow.

The workshop featured a presentation on the legal framework by the European Commission, followed by a panel including presentations from the perspectives of health data holders (industry, academia), HDABs and health data users. These presentations all framed and brought input to the following session where participants were asked to discuss IP rights and trade secrets in regard to five steps in the secondary use workflow: 1) Metadata communications, 2) HDAB assessment of data access requests, 3) data provision, 4) analysis within secure processing environments (SPEs), and 5) export and disclosure of results.

Introduction

This workshop marks the third and final workshop of a series under TEHDAS2 Work Package 4, which focuses on developing collaboration models for the EHDS. The workshop series has been structured around three main topics: 1) Ethics, 2) collaboration models, and 3) IP rights and trade secrets. Taken together, these workshops are designed to involve key stakeholders, promote transparency, and produce practical policy recommendations that will support the effective implementation of the EHDS.

Session 1: Setting the scene on the legal framework for IP rights and trade secrets under the EHDS

Presentation: Guillaume Byk, Policy Officer, DG SANTE

The EHDS seeks to balance the protection of IP rights, regulatory data protection and trade secrets with the legitimate interests in enabling secondary use of health data. While it does not diminish or bypass existing legal protections, it establishes a framework that enables controlled access to data while maintaining these rights.

Key legal provisions

Under Article 52, data sets protected by IP rights, regulatory data protection or trade secrets may be made available for secondary use, provided that health data holders notify HDABs of any protected elements. HDABs must ensure legal, organisational and technical safeguards, and they may impose conditions such as contractual agreements or refuse access if adequate protection cannot be guaranteed. To support their task, the European Commission will issue non-binding model contractual terms of arrangements between health data holders and users.

Types of rights and assessment approach

As the EHDS does not define a closed list of applicable rights, multiple forms of protection may apply, including database rights, copyright, patents, regulatory data protection and trade secrets. Given the diverse nature and duration of these rights, HDABs must assess data access requests on a case-by-case basis, considering the type of data its intended use and the identity of the applicant. Data Holders must also notify HDABs of any update in the protection status of datasets, for example due to patent expiry.

Safeguards and operational considerations

Health Data holders are expected to flag protected elements when submitting dataset descriptions during permit procedures or when the data is requested at the latest. HDABs may apply various safeguards, including confidentiality obligations, organisational measures such as removing sensitive elements, and technical restrictions within secure processing environments. Protection of IP rights, regulatory data protection and trade secrets must be upheld throughout the entire data lifecycle including access, processing, publication of results and export of anonymised data.

Redress and remaining operational questions

Both Health Data Holders and users may file complaints with HDABs regarding access decisions, which can subsequently be challenged in national courts. Existing IP, trade secrets and regulatory data protections regimes are not affected and continue to apply fully under the EHDS. However, several practical questions remain unsolved, including which datasets will be affected, which safeguards are most effective, and when access should be granted with conditions or refused altogether.

Q&A

Q: How can the three-month deadline for HDAB decisions be reconciled with complex case-by-case assessments of datasets containing IP rights or commercially sensitive information?

A: The timeline is set in the Regulation and offers limited flexibility, but guidance from the EHDS Board may help streamline common cases.

Q: How scalable will the assessment process be, particularly in cross-border requests where several national HDABs may be involved?

A: It was clarified that assessments remain national; different HDABs may reach different decisions, although the EHDS Board is expected to support greater consistency.

Q: Will data holders be informed about protection measures proposed by HDABs, and will they have the possibility to challenge these measures?

A: Dialogue with data holders is expected. Complaints and legal remedies remain available.

Q: How will the EHDS data catalogue be designed, and will datasets be searchable by data holder?

A: Searchable metadata fields and flags for protected elements are expected, although details are still under development.

Q: How can trade secrets be identified already at the catalogue stage, given that many datasets may potentially contain confidential elements?

A: Early notification helps HDABs anticipate protection needs, although practical approaches may still need to be developed.

Q: How will HDABs ensure sufficient expertise when assessing IP rights and trade secrets, particularly where data holders may have the most detailed knowledge of the data?

A: There will be a dialogue with data holders. HDABs remain responsible for final decisions.

Q: How should trade secret protection be assessed in relation to the purpose of a data access request?

A: Assessments will be made case by case, considering the type of data, the applicant, and the intended use.

Session 2: Stakeholder needs and expectations

Presentation: Simon Bates, Senior Director of Patent Law, Johnson & Johnson, UK

Health data holder, industry

The industry continues to act as a cornerstone in supporting the EHDS, recognizing its transformative potential to accelerate scientific progress and foster health innovation. However, this support is tempered by significant concerns regarding IP rights and the protection of trade secrets, which remain critical to maintaining competitive advantage and encouraging ongoing investment in research and development.

The importance of robust IP safeguards cannot be overstated. Effective IP protection not only supports innovation but also ensures that DUs and DHs can operate within a secure and predictable framework. Without such protections, the risk of unintended exposure of sensitive information, whether through device-generated data, proprietary algorithms, or clinical trial results, could undermine trust and collaboration across the sector.

The pharmaceutical sector faces several risks, including the risk of exposing sensitive clinical trial data, which could compromise both competitive positioning and patient confidentiality. For the MedTech industry, key challenges include the handling of device-generated data and proprietary algorithms, as well as persistent uncertainty about disclosure obligations under the EHDS. Additionally, the challenges posed to the MedTech industry cannot be viewed as isolated to the EHDS. For example, the combined effect of the Data Act and EHDS regulation could fundamentally challenge the proprietary nature and competitiveness of MedTech products and services by creating data access risks that enable reverse-engineering, undermine innovation investment, and potentially compromise patient safety.

In response to these challenges, the industry is actively considering what successful EHDS implementation would entail.

Central to this vision are six foundational principles:

- Dedicated IP and trade secret task forces within HDABs to provide expert oversight and address IP-related challenges.
- Enable health data holders to indicate confidentiality levels and access conditions, ensuring data providers retain control over their sensitive information.
- Establish best practices around existing legal, organizational, and technical safeguards, to create a clear, actionable framework for all stakeholders.
- Involve experts who understand dataset sensitivity throughout the data user journey, to prevent misuse and ensure appropriate handling of sensitive data.

- Clear delineation of the scope of data categories under Article 51, to avoid ambiguities and ensure consistent application.
- Clarify complaint and liability mechanisms, to provide transparent, accessible procedures for raising concerns and seeking redress.

To guide these efforts, a 3Cs framework has been proposed: clarity to eliminate ambiguity, consistency to align practices across the EU, and certainty to provide a stable and reliable environment for all participants.

In parallel, the IHI project consortium has advanced to the grant preparation phase, with details remaining confidential. Recommendations arising from this initiative will be informed by high-quality input from ongoing discussions, aiming to address the most pressing challenges identified by industry stakeholders.

The desired outcomes of the workshop include the identification and agreement on the 3Cs framework, fostering mutual understanding among participants, and achieving a balanced, harmonized, and consistent approach to EHDS implementation.

Presentation: Johan Van Eldere, Secretary-General, European University Hospital Alliance, Belgium

Health data holder, academia

In the context of IP rights and trade secrets, EUHA advocates for a balanced approach between openness and protection, rejecting centralized data warehousing in favor of a federated governance model based on secure access rather than data transfers. This model relies on processing within controlled environments, with full traceability, logging, and federated validation infrastructures across institutions, while preserving GDPR-aligned data controllership at the institutional level.

EUHA highlights that much of the data used in research originates from academic projects rather than primary care, and that hospitals invest significantly in structuring electronic health records, curating and annotating data, and ensuring quality and interoperability. These efforts embed substantial clinical know-how in registries and biobanks, which constitute protected assets under database rights and trade secret frameworks. Therefore, any secondary use of health data must respect intellectual property rights, database rights, and trade secrets, as well as the legitimate confidentiality interests of data holders. Open science, in this view, does not imply unrestricted commercial reuse or loss of control over derivative outputs, and proportionate compensation mechanisms and governance agreements should remain possible.

The alliance also stresses the importance of attribution and academic recognition, arguing that excluding originating institutions from data analysis risks loss of context, reduced reliability, and weakened incentives for maintaining high-quality datasets. EUHA calls for mandatory attribution, robust provenance tracking, recognition of dataset creation as a research output, and transparent feedback on secondary uses, in line with international authorship standards. More broadly, EHDS implementation should reinforce data stewardship cultures rather than commoditize hospital-generated data.

Regarding reuse, EUHA supports strict safeguards, including a clear legal basis such as public interest research, the use of secure and validated environments, and the inclusion of contextual metadata to preserve data quality. Additional requirements should include bias testing, representativeness assessments, post-market monitoring with feedback loops to originating institutions, transparency in commercial uses, and governance agreements that clarify responsibilities. Importantly, liability for downstream AI systems developed by third parties should not be shifted onto data-originating hospitals.

EUHA positions health data holders as structural actors within the EHDS, advocating for their continued role as primary data controllers under GDPR, active participation in governance networks and federated AI validation infrastructures, and recognition as ethical gatekeepers, particularly in post-market validation processes. Hospitals, in this perspective, must not be reduced to passive data providers.

In conclusion, EUHA calls for an EHDS implementation that ensures federated and secure access to data, preserves institutional controllership, and protects intellectual property and clinical know-how, while also introducing mandatory attribution, recognition and compensation mechanisms, strong safeguards for AI-related reuse, and clear liability boundaries. It ultimately rejects any perceived conflict between open science and IP protection, promoting instead a balanced framework that supports innovation, transparency, and societal benefit while safeguarding institutional interests

Presentation: Inge Franki, EU Unit manager, Health Data Agency, Belgium

Health data access body

Belgian Health Data Agency, represented by Inge Franki, highlights that HDABs are still in the process of developing and several member states are still in the process of nominating and establishing an HDAB. Within that process, is the development of an approach for the assessment of IP and trade secrets, forming only one component of a broader set of responsibilities. The Belgian HDA itself has already taken initial steps by launching discussions through multi-stakeholder working groups, organizing workshops with medtech associations, and developing training initiatives such as the HDAcademy to improve private sector understanding. It is also actively engaging with European partners, including through Digital Europe initiatives, while preparing technical tools to manage IP-related challenges.

From a technical standpoint, the HDA is integrating IP considerations into its infrastructure. The HDA is considering the possibility that its metadata catalogue could allow certain sensitive metadata to be hidden, while standards such as Health DCAT-AP already include fields to flag IP-related constraints. Data access application and request forms already enable applicants to indicate whether datasets are subject to IP protection and to provide explanations. At the same time, automated links to transparency portals include mechanisms to restrict the transfer of sensitive information where necessary.

However, significant operational challenges remain. Regarding data descriptions, the requirement under Article 52 to notify datasets to an HDAB raises practical difficulties, as notification at the stage of an actual request may come too late to allow for a thorough assessment of protection measures. This points to the need for a clearer and more harmonized operational framework. In terms of data provision, technical measures under Article 52(3) still require detailed analysis, and stronger

collaboration between HDABs is needed. Legally, current frameworks provide limited authority for HDABs to request the documentation necessary to assess IP protections, highlighting the need for a clearer legal basis, including rules on confidentiality and secrecy obligations that would enable HDABs to perform their role effectively. Similarly, transparency requirements around data access requests require clearer guidance, particularly regarding the publication of outcomes.

More broadly, several structural issues complicate the implementation of IP safeguards. The definition of data holders remains under discussion, while the geographical location of legal entities could create inconsistencies or opportunities to circumvent the EHDS framework. The assessment of patents may be relatively straightforward, but evaluating trade secrets is considerably more complex and context-dependent.

In conclusion, while robust assessment of IP and trade secret protections is essential, it remains highly challenging in practice. There is a clear need for a common and possibly harmonized European framework, supported by structured decision-making tools, while still allowing for necessary case-by-case evaluations. This, however, increases complexity and requires both sufficient capacity and specialized expertise within HDABs. Strengthened collaboration between HDABs at the European level, along with continuous dialogue and awareness-building between HDABs and data holders, is seen as essential to ensuring an effective and balanced system.

Presentation: Pedro Ramos, Researcher, Karolinska Institutet, Sweden

Health data user

Karolinska Institutet, represented by Pedro Ramos, approaches the question of IP rights and trade secrets in the EHDS from the perspective of health data users, emphasizing the need to safeguard innovation in the secondary use of health data while accounting for the diversity of user profiles. These include academic and clinical researchers, multi-partner research consortia such as those funded under Horizon programmes, public authorities, innovation-driven SMEs, and research infrastructures, all of whom have distinct needs that the EHDS framework should reflect.

A key concern relates to the growing complexity and bureaucratic burden associated with IP-related processes, particularly for academic researchers. There is a risk that these requirements could contribute to the emergence of a two-tiered system, where well-funded institutions are better equipped to navigate data access and IP constraints, while smaller research groups face increasing barriers. IP considerations may also introduce hidden costs at the stage of data discovery, further exacerbating inequalities. At the same time, the EHDS implies a shift in research practices, as researchers will need to operate within SPEs, a model with which many are unfamiliar. This raises practical challenges, including limited experience with output restrictions, documentation requirements, and emerging IP issues, particularly in relation to AI and generative AI use cases.

In response, capacity building is identified as a critical prerequisite for responsible access to data within SPEs, requiring coordinated efforts at multiple levels. The intervention also highlights that data users are often simultaneously data holders, which creates cultural and operational tensions between the goals of transparency and controlled access. This is particularly evident in scenarios involving curated registries, enriched datasets, multi-source data linkages, temporal protection mechanisms, and expectations around recognition for value-added contributions.

From an IP perspective, several critical dimensions arise throughout the data use lifecycle, including the exposure of sensitive elements at the application stage, the protection of research outputs, questions around ownership of derived data, and the growing importance of AI and algorithm-related IP. Finally, there is a need to ensure alignment between the EHDS framework and existing multinational research initiatives, so as to avoid fragmentation and support coherent innovation ecosystems.

Panel debate moderated by Nienke Schutte, Sciensano, Belgium

How feasible is it for data holders to identify IP-rights and trade secrets in datasets, particularly at the metadata stage?

The feasibility of identifying IP-rights and trade secrets at the metadata stage varies significantly depending on both the dataset and the data holder. As a good practice, dataset can be flagged as IP-sensitive in their descriptions, although in some cases a detailed, case-by-case assessment may still be required. One of the speakers emphasised that clinical datasets often make it difficult to isolate specific IP-protected elements, which may argue for broader protection of electronic health records under IP or trade secrets frameworks. It was further highlighted that publicity funded datasets should ensure a return to the public interest when downstream value is created, with advanced therapy medicinal products serving as an example that relies heavily on publicly funded clinical registries.

Can trusted data holders help address cross-border challenges in EHDS, and what role should HDABs play?

Trusted data holders can support the handling of cross-border challenges in the EHDS by offering guidance and documentation, but a speaker also underlined that, the ultimate responsibility for decisions must remain with HDABs, whose capacity will need to be reinforced. Effective cross-border coordination requires structured collaboration between HDABs to ensure consistent evaluation of protection mechanisms, supported by common operational procedures developed bottom-up thought their joint efforts. Initiative such as the Community of Practice and the EHDS-board can further facilitate coordination and the exchange of practical experience across Member states.

How can EHDS ensure clarity and predictability for researchers without discouraging legitimate scientific research?

Ensuring clarity and predictability for researchers under the EHDS requires recognising that health data users represent diverse research personas with differing incentives and needs, as highlighted by a speaker. While the EHDS has the potential to greatly improve access to electronic health records, especially for researchers who currently lack established access pathways – uncertainty about the availability and usability of datasets may discourage them from relying on EHDS catalogues. At the same time, IP considerations are particularly significant for research groups engaged in spin-offs or commercialisation activities, which can create tensions within academic environments. Achieving predictability therefore requires transparent information on dataset accessibility and clear guidance on IP implications, without introducing barriers that limit legitimate scientific research.

Need for a common operational framework for EHDS implementation

A common operational framework for implementing the EHDS requires a bottom-up collaborative approach among stakeholders, as emphasised by one of the speakers, who noted that practical progress should not wait for legislative mandates. From the HDAB perspective it was also highlighted that the EHDS framework is already established, underscoring the importance of joint initiatives and EU-supported projects to develop workable implementation models. From the academia perspective it was pointed out that differing interpretations of EU legislation across member states continue to pose significant barriers, particularly for cross-border research, reinforcing the need for greater harmonisation. A Commission representative supported this collaborative bottom-up approach, noting that stakeholders should contribute to develop practical solutions while the EHDS board will provide a governance structure to guide common practices and promote harmonised implementation across Member states.

Session 3: Operationalising IP and Trade Secret protection in the EHDS secondary use workflow

Session 3 consisted of interactive group discussions structured around five key stages of the EHDS user journey for secondary use. Participants discussed practical challenges and possible solutions, and groups subsequently presented their key insights to the plenary.

The discussions aimed to identify legal, organisational, and technical measures across the different stages of the secondary-use process to inform future EHDS implementation.

1: Metadata communications (pre-access stage)

Scope: *How IP and trade secret relevant information is communicated at the metadata stage, ensuring that metadata is sufficiently informative for data discovery and request formulation, without inadvertently disclosing sensitive or commercially confidential information.*

Key discussion points

Participants agreed that dataset discoverability is crucial for helping data users identify relevant data. However, metadata must be designed so it does not reveal commercially sensitive information, trade secrets, or the identity of data holders. There is also a need for clearer and more transparent criteria for how access decisions are made and what metadata is required. In addition, discussions highlighted that metadata should be understood as part of a broader continuum of the EHDS secondary use process, rather than an isolated step. This implies that considerations around IP protection, data holder interests, and user needs should already be reflected at this early stage and remain consistent throughout the workflow. Participants also stressed that increasing transparency, particularly regarding how HDABs assess requests and apply criteria, would help build trust in the system. More detailed and operationalised criteria, potentially embedded in a common EU-level framework, were seen as important to ensure predictability and fairness, including in situations involving competitors or commercially sensitive data uses.

Challenges and concerns

Metadata can unintentionally expose sensitive information, including valuable insights or the identities of data holders. Even listing dataset variables may reveal proprietary knowledge. Some trade secrets only become apparent after extensive analysis, leading to arguments that data holders should have time to exploit their data before metadata becomes public. There were also concerns that metadata could enable indirect identification of data holders or sensitive entities, creating risks related to competitiveness or strategic positioning. Another key concern relates to the lack of sufficiently detailed and harmonised criteria for access decisions, which may weaken trust in the system. In particular, current guidance was seen as not always adequately accounting for factors such as the relationship between data users and data holders (e.g. potential competitors). Finally, participants noted a tension between the need for rich metadata to support discoverability and the risk of revealing too much information, especially in cases involving rare diseases or highly specific datasets.

Suggested solutions and examples

Proposed solutions included:

- Greater transparency on decision-making criteria, including more detailed and operational guidance on how HDABs assess access requests;
- Embedding criteria within a common legal or governance framework at EU level to ensure consistency and trust;
- Use case-based approaches (e.g. rare diseases, synthetic data, specific data categories) to illustrate how metadata can be sufficiently informative while protecting IP and trade secrets;
- Development of a shared toolkit or checklist, accessible to HDABs, data holders, and data users, to support consistent and objective implementation across Member States;
- Continuous involvement of data holders, as of early stages, to validate that metadata does not inadvertently disclose sensitive or commercially valuable information.

2: HDAB assessment of data access requests (decision-making stage)

Scope: *How HDABs assess and manage IP and trade secret risks alongside privacy, public interest, and usability considerations, particularly in cross border, multi country, and large-scale requests, and how consistent decision making can be ensured across the EHDS*.

Key discussion points

A central theme was the role of HDABs in balancing data access with the protection of IP and trade secrets. Participants highlighted the importance of structured collaboration between HDABs and data holders during assessments and stressed the need for multidisciplinary expertise within HDABs, including IP and trade secret law, data protection, technical infrastructure knowledge, and sector-specific insight. Beyond assessment, HDABs were also seen as facilitators or mediators between data holders and data users. Participants emphasised that structured dialogue mechanisms should be in place to ensure that relevant information, particularly regarding IP sensitivities and risks, is communicated early and effectively. Without such interaction, there is a risk of misunderstandings, increased legal uncertainty, and potential disputes or litigation. Harmonised decision-making across Member States was seen as essential for ensuring consistency and trust in cross-border requests. This includes not only common criteria, but also shared tools, aligned interpretations, and mutual trust between HDABs, given that they will rely on each other's decisions in cross-border contexts.

Participants also highlighted the importance of clearly defining roles and responsibilities, including the responsibility of data holders to justify and substantiate claims that data are protected by IP or trade secrets. Objective evaluation criteria and adequate documentation from data holders may therefore be needed to determine whether such claims are justified. Finally, discussions pointed to the importance of timing considerations, as the value of data from an IP perspective may evolve over time. This reinforces the need for early communication and clarity during the assessment phase.

Challenges and concerns

Concerns were raised about whether HDABs can attract and retain the required expertise. There is limited clarity on how to assess risks related to IP, trade secrets, and the definition of "serious risk", which may lead to inconsistent decisions across Member States. Some stakeholders, especially industry, expressed limited trust in authoritie's ability to safeguard sensitive data. This highlights the need to demonstrate both technical robustness and institutional capacity within HDABs. Assessing the validity of IP or trade secret claims may additionally require documentation and clear tools that are currently lacking. At the same time, there is a tension between ensuring sufficient expertise and avoiding overly complex or resource-intensive systems that only some Member States could implement. A further challenge relates to the lack of structured communication mechanisms between HDABs and data holders, which may lead to uncertainty, inefficiencies, or increased risk of appeals. Finally, ensuring harmonisation across Member States remains difficult, particularly given differences in capacity, interpretation of legal concepts, and availability of expertise.

Suggested solutions and examples

Suggested solutions included developing templates, guidance, or toolkits to support consistent assessments and improve communication around IP-related risks. Participants proposed establishing a reference centre or helpdesk to offer legal and technical support, as well as creating objective criteria and practical tools to enable evidence-based decisions. There was strong support for structured consultation mechanisms between HDABs and data holders, particularly at the early stages of the assessment process, to ensure that IP and trade secret considerations are properly understood and addressed.

Participants also emphasised the need for:

- Clear governance frameworks and legally grounded criteria to guide decision-making across the EU;
- Harmonised tools and processes to support consistency and mutual trust between HDABs;
- Active involvement of stakeholders (e.g. EHDS Board, stakeholder forum, community of practice) in developing and refining these tools;
- Risk-based approaches, such as triaging requests into low-, medium-, and high-risk categories, with corresponding levels of scrutiny and expertise required;
- Capacity-building measures, including guidance, shared resources, and potentially centralised expertise, to support HDABs with limited resources.

Greater transparency in evaluation criteria was seen as key to improving predictability and trust. Ensuring multidisciplinary expertise within HDABs and promoting structured consultation with data holders were also recommended.

3: Data provision (data preparation and transfer stage)

Scope: *Safeguards applied when data are prepared and transferred from the data holder to the HDAB or SPE, including contractual, technical, and organisational measures.*

Key discussion points

This stage received relatively limited discussion compared to earlier phases. Participants noted that when trust, safeguards, and the data permit are properly established earlier in the process, the later steps tend to be more manageable. In particular, the discussion highlighted a sequential and conditional approach to risk management: if robust assessment, clear criteria, and effective communication with data holders are ensured in earlier stages, the need for additional safeguards during data provision is reduced. Participants therefore viewed this phase as operational rather than decision-heavy, with the assumption that key risks related to IP and trade secrets should already have been addressed upstream.

Challenges and concerns

A key challenge identified was clarifying the division of responsibilities between data holders and HDABs when preparing and transferring datasets. More broadly, there is a need to ensure that the safeguards agreed during the assessment phase are correctly implemented in practice during data preparation and transfer, particularly in relation to protecting IP-sensitive elements of datasets. Although not extensively discussed, this stage also implicitly depends on the existence of clear standards and procedures for secure transfer and preparation, without which inconsistencies may arise across Member States.

Suggested solutions and examples

One solution proposed was for the HDAB to conduct the analysis itself and provide only summary statistics to the data user, rather than granting access to raw data. This approach was mentioned as a potential way to reduce risks related to trade secrets and intellectual property. This reflects a broader approach of minimising exposure to raw data where possible, by shifting certain analytical functions upstream to trusted actors within the EHDS infrastructure.

Participants did not identify many additional safeguards specific to this stage, reinforcing the view that effective upstream governance, clear data permits, and strong SPE requirements are the primary mechanisms for managing IP and trade secret risks.

4: Analysis within Secure Processing Environments (use and analysis stage)

Scope: *How SPEs may support the protection of IP and trade secrets during analysis, while remaining functional and attractive for research and innovation.*

Key discussion points

Secure Processing Environments (SPEs) were viewed as a key safeguard for protecting IP rights and trade secrets during data analysis. Participants emphasised that this is the stage “where the data are actually accessed and used,” and therefore where protection mechanisms are most critical. SPEs were described as the core technical environment where trust must be operationalised, as they are the point at which third parties interact directly with potentially sensitive data. Participants

noted that many implementation details are still under development, particularly concerning requirements to be defined in upcoming implementing acts. As a result, expectations around SPE functionality and safeguards remain partly uncertain.

Challenges and concerns

Concerns were raised about cybersecurity risks, such as hacking, that could undermine trust among citizens and industry stakeholders. These risks were perceived not only as technical issues but also as key barriers to trust and participation in the EHDS ecosystem. There is also limited clarity regarding the specific technical safeguards that SPEs will be required to implement, contributing to uncertainty among stakeholders. In addition, participants highlighted the need to ensure that user behaviour within SPEs is appropriately controlled and monitored, given that risks to IP and trade secrets may arise during data use rather than only from data access itself.

Suggested solutions and examples

Suggested measures included strong monitoring and logging of authorised users and their activities within SPEs, including tracking who accesses data and how it is used. This was seen as a key mechanism for ensuring accountability and preventing misuse. Participants also emphasised the importance of:

- Robust technical safeguards within SPEs, aligned with high security standards;
- Clear communication from authorities about these safeguards, particularly through upcoming implementing acts, to reduce uncertainty and build trust;
- Transparency regarding security measures, to reassure both data holders and data users that IP and trade secrets are adequately protected.

Overall, strengthening both the actual security and the perceived reliability of SPEs was seen as essential to ensure their acceptance and effective use within the EHDS framework.

5: Export and disclosure of results (post-analysis stage)

Scope: *How outputs derived from secondary use are reviewed, exported, disclosed, or published without compromising IP or trade secrets, while respecting transparency and accountability requirements.*

Key discussion points

Participants highlighted the role of HDABs as facilitators, especially when analyses involve multiple datasets and data holders. In such cases, HDABs are expected to ensure that the export of results respects the conditions set in the data permit and that all relevant constraints are consistently applied. It was also emphasised that exported results must remain within the scope of the data permit and avoid disclosing any confidential information. The data permit was seen as a key instrument for defining the boundaries of acceptable outputs, including permitted purposes and limitations on disclosure. Participants also highlighted the importance of traceability across the full data lifecycle, including understanding what happens after results are exported, such as how data contributes to publications, further research, or innovation outcomes.

Challenges and concerns

There is a risk that results or summary outputs may unintentionally reveal sensitive or commercially confidential information. This concern extends not only to raw outputs but also to aggregated or derived results, which may still contain implicit insights. Uncertainty remains regarding how publication requirements, such as the 18-month publication rule, interact with contractual agreements between data holders and users. Participants questioned whether and how such obligations could be reconciled with IP protection or commercial interests. Questions were also raised about how to ensure that data are used strictly for the permitted purposes, including concerns that results could be used to develop competing products or generate unintended commercial advantages. More broadly, participants noted that overly restrictive frameworks or unclear rules at this stage could discourage both data holders and data users from engaging with the EHDS, highlighting the importance of maintaining a balance between protection and usability. Finally, questions remain regarding the ownership of intellectual property generated through research using EHDS data, particularly in multi-actor or cross-border contexts.

Suggested solutions and examples

Participants suggested building on existing models for secure result export used in regulatory and research infrastructures, rather than developing entirely new approaches. Developing clear and transparent criteria for reviewing outputs before release was identified as essential to ensure that no confidential or sensitive information is disclosed. This includes defining what can be included in summaries, publications, or other outputs.

Participants also recommended:

- Strengthening monitoring mechanisms to ensure that results are used in line with the permitted purposes;
- Improving traceability of research outcomes, to better understand how data contributes to publications, discoveries, and innovations;
- Clarifying rules around publication and disclosure, including how legal obligations interact with contractual arrangements and IP protection;
- Leveraging existing best practices and technical solutions for controlled result export and disclosure.

These measures were seen as important to ensure both protection of IP and trade secrets and continued attractiveness of the EHDS for research and innovation.

Final reflections on session 3

Across the different stages of the EHDS user journey, trust, transparency, and clear governance mechanisms were repeatedly highlighted as key conditions for successful implementation. Participants emphasised that these elements must be ensured consistently across the entire workflow, rather than addressed in isolation at specific stages. The EHDS was therefore seen as a continuum, where decisions and safeguards in earlier phases directly shape the feasibility and risk profile of later steps. Effective collaboration between data holders, data users, and HDABs emerged as a central requirement. In particular, the need for structured dialogue and early involvement of data holders was highlighted as critical to managing IP and trade secret risks, avoiding misunderstandings, and reducing the likelihood of disputes. At the same time, HDABs were expected

to play a facilitating and mediating role, requiring both sufficient expertise and clearly defined responsibilities. Participants also stressed that trust is not only a matter of legal compliance, but also of demonstrable technical safeguards and predictable decision-making. This includes transparency in evaluation criteria, clarity on roles and processes, and confidence in the security and governance of infrastructures such as Secure Processing Environments. Without such assurances, particularly industry stakeholders, there is a risk of limited participation in the EHDS. A recurring theme was the need to strike a balance between protection and usability. While robust safeguards for IP rights and trade secrets are essential, overly complex, restrictive, or unclear frameworks may discourage both data holders and data users from engaging. This highlights the importance of designing processes that are not only secure, but also operational, proportionate, and attractive for research and innovation. Finally, participants underlined the importance of harmonised guidance, practical tools, and shared frameworks at EU level, including templates, toolkits, and common criteria to support consistent implementation across Member States. Such elements were seen as essential to ensure that IP rights and trade secrets can be safeguarded while still enabling meaningful secondary use of health data under the EHDS.

Future outlook

The perspectives set out in this workshop report will feed into one of the work of the public private IHI Fortify consortium, which will start to work in June 2026. It remains to be seen how these perspectives will be reproduced at national and EU-level. This report should therefore be closely considered both by the EHDS Board and the Community of practice EHDS2.