bitkom

Position paper

Bitkom detailed comments for the European Health Data Space (EHDS)
March 2023

Malte Fritsche
Policy Officer Health & Pharma

T +49 30 27576-404
m.fritsche@bitkom.org

Albrechtstraße 10
10117 Berlin

General Remarks

As Bitkom, we put forward our general comments on the Commission's proposal for the European Health Data Space in a first position paper in July 2022. As the discussions on the text are ongoing in Council and Parliament, we want to further elaborate on certain points to provide constructive criticism during this process. In the following, we therefore give a more detailed assessment of certain articles and concepts within the European Health Data Space that also picks up specific wording.

Chapter I: General provisions

Definitions

EHR system definition clarification
Considering the mode of operation of medical devices, the current definition of EHR system is so broadly defined that almost all medical devices would always also be EHR systems which does not seem to be the intent of the Commission's proposal. The definition should be adapted by, at least as a starting point, adding the wording 'primarily intended by the manufacturer' to prevent that a secondary aspect (namely processing of electronic health data) renders a medical device (the primary intended use of which is as defined in Regulation (EU) 2017/745) into an EHR system. (our proposals in **blue**)

Article 2.2

(n) 'EHR system' (electronic health record system) means any software **primarily** *intended by the manufacturer to be used for storing, viewing and sharing of electronic health records, whose main purpose is to facilitate sharing patient information with authorized providers, healthcare professionals, or patients and to a data flow between healthcare facilities;*

Data holder definition clarification

The distinction between Data holder and data processor is vague and creates risks of noncompliance with GDPR. Legal clarity and alignment with the GDPR for sufficient data protection is needed to ensure clarity who is a data holder under the EHDS.

Also, the definition of data holder should be aligned with the Data Governance Act to avoid confusion in situations where both regulations may apply.

Article 2.2

(y) 'data holder' means any natural or legal

person, which ~~is an entity or a body in the health or care sector, or performing research in relation to these sectors, as well as Union institutions, bodies, offices and agencies who has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation implementing Union law, or in the case of non-personal data, through control of the technical design of a product and related services, the ability to make available, including to register, provide, restrict access or exchange certain data~~

- ***a Union institution, body, office, or agency, or,***
- ***an entity or a body in the health or care sector, or performing research in relation to these sectors and,***
- ***is a data controller, or,***
- ***has the right or obligation, in accordance with this Regulation, applicable Union law, or national legislation implementing Union law, or in the case of non-personal data, through control of the technical design of a product and related services, or the ability to make available, to register, provide, restrict access or exchange electronic health data pursuant to this Regulation.***

Further changes and new clauses for Article 2 to clarify specific definitions

The definition of 'electronic health data' in the proposal includes both personal and non-personal electronic health data. These concepts are indispensable not only to define the scope of the legislation but also for its objective to make the re-use of health data more effective. Further clarity is needed especially on the concept of 'non-personal electronic health data' which is open to broad interpretation due to various applications of the GDPR and health data processing rules in Member States. Where non-personal electronic health data means health and genetic data in electronic form that fall outside of the definition of personal data under the GDPR, it would mean that only anonymized data will be available for download to the data user under the EHDS. Considering that the effectiveness of anonymization of e.g., medical images is being questioned, medical images may never become available for download, blocking the training, testing and evaluating of algorithms, which is part of the intent of the EHDS as pointed out in its Recital 41. Similar types of electronic health data may experience the same limitations.

In this regard, the EHDS proposal should be supported by long-overdue updated guidelines from the European Data Protection Board on the concept of personal and non-personal data and and on anonymization/pseudonymization techniques, as well as scientific research to ensure legal certainty for stakeholders on what impact the EHDS might have on different datasets.

Article 2.1

(a) the definitions ***of "controller" and "processor"*** *in Regulation (EU) 2016/679*

(...)

(g) The definition of 'critical infrastructure' pursuant to art 2 (4) of European Parliaments legislative resolution of 22 November 2022 on resilience of critical entities.

Article 2.2

(b) "non-personal electronic health data" means data ~~*concerning*~~ ***constituting*** *health and genetic data in electronic format that falls outside the definition of personal data provided in article 4(1) of regulation (EU) 2016/679;*

'Interoperability' definition clarification

It is unclear what is meant by 'mutually beneficial goals'. We suggest using the definition of 'interoperability' in the Medical Device Regulation where devices work together as intended.

Article 2.2

(f) 'interoperability' means the ability of ***two or more devices, including software*** ~~*organisations as well as software applications or devices*~~ *from the same or different manufacturers,* ***to*** ~~*interact towards mutually beneficial goals, involving the*~~ *exchange* ~~*of*~~ *information and* ~~*knowledge without changing the content of the data between these organisations, software applications or devices, through the processes they support;*~~ ***use the information that has been exchanged for the correct execution of a specified function without changing the content of the data, and/or communicate with each other, and/or work together as intended****.*

'Economic operator' definition

EHR systems may be deployed by the manufacturer, the user or a third party, contracted by the manufacturer or user to deploy and maintain the system. Therefore, to ensure that responsibilities and obligations by all parties involved in the EHR system's deployment and use are fully covered, a definition should be introduced to reflect all possible scenarios in practice and deploy Article 16 effectively.

Article 2.2

(af) 'economic operator' is a natural of legal entity which deploys and maintains technical characteristics of the EHR system in the healthcare sector.

Article 2.2

(q) 'serious incident' means any malfunction or deterioration in the characteristics or performance of an EHR system made available on the market that directly ~~*or indirectly*~~ *leads or* ~~*might have led*~~ ***has*** *led* ~~*lead*~~ ***to*~~ *any of the following*~~*:*

(i) the death of a natural person or serious damage to a natural person's health;

(ii) a serious disruption of the management and operation of critical infrastructure in the health sector;

'Online pharmacies' definition clarification

Bitkom welcomes the mention of online pharmacies in the draft text, especially in Article 12, which contributes to the creation of a level playing field of different healthcare providers, online and offline. Since there is currently no definition of online

pharmacies in previous legal acts, we suggest that they be supplemented within the framework of Article 2 of the draft.

Article 2.2

(ag) 'Online pharmacy' means a pharmacy legally established as such in a Member State for which a pharmacist within the meaning of Directive 2005/36/EC is responsible, which, by means of information society services directed to the public (i) dispenses prescriptions and/or (ii) offers medicinal products for sale and/or (iii) provides other pharmaceutical services.

Chapter II: Primary use of electronic health data

Timeframe to access electronic health data

Technical feasibility shall be factored in, and thus reasonable timeframes should be judged acceptable for providing access to one's health data and the healthcare providers and professionals accessing one's health data. In addition, when setting up procedures for fulfilling data requests from individuals, Member States should ensure that there is no excessive fragmentation of the process, for instance through guidelines. For instance, the request for data should not have to be processed by manufacturers holding health data as processors.

Article 3.1

*1. ~~Natural persons~~ **Individuals** shall have the right to access their personal electronic health data processed in the context of primary use of electronic health data, ~~immediately~~ **within a reasonable timeframe**, free of charge and in an easily readable, consolidated and accessible form.*

Article 3.10

*~~Natural persons~~ **Individuals** shall have the right to obtain information on the healthcare providers and health professionals that have accessed their electronic health data in the context of healthcare. The information shall be provided **within a reasonable timeframe** ~~immediately~~ and free of charge through electronic health data access services**, in line with Article 15 of Regulation (EU) 2016/679**.*

Health data access services openness to third party applications

Patients should be able to access and feed their electronic health records via the health data access services directly and via the digital health services, products and applications they already use regularly for managing their health. The interfacing of digital health services with electronic health records should be conditioned by explicit patient consent and the compliance of these services with strict security and confidentiality rules. Furthermore, Member States' electronic health data access services should interface to similar services complementing the services provided by the Member States. Such additional services may be beneficial to the general public and enable the private sector to offer innovative concepts to the individuals.

To generate acceptance of the data processing of electronic health data, consent should be the primary source of authorization for such processing. This enables patients to exercise autonomy regarding their health affairs and thus ensures the necessary buy-in for new technology. In order to avoid fears of being overwhelmed and out of control of their own health data, patients need to be assured that the data processing only occurs with their consent and thus voluntarily.

Article 3.5

Member States shall:

(...)

(c) allow electronic health data access services to interface with digital health services, other electronic health data access services, products and applications under strict security, confidentiality and consent conditions. Security and confidentiality requirements allowing digital health services to interface with electronic health records should be defined by member states. The interfaces should follow the European Interoperability Standards aligned with requirements defined in Article 23.

Patients' interactions with national health data access services

Patients should be able not only to "insert", but also to "access" and "transfer" their electronic health data in their EHR using "applications linked to these services".

Article 3.6

*~~Natural persons~~ **Individuals** may insert**, access and export** their electronic health data in **and from** their own EHR or in that of natural persons whose health information they can access, through electronic health data access services ~~or~~ **and** applications linked to these services. That information shall be marked as inserted by the natural person or by his or her representative.*

International standards

International standards should be referred to and followed by the Member States. Reference to the EU recommendation 2019/243 is also proposed. Some of the reasons why it is important:
1. Achieving technical and semantic interoperability and seamless exchange of data and information is critical to the success of the European Health Data Space and improvements in clinical operations, patient outcomes and cost of healthcare. The interoperability of electronic health records, in line with the existing European Electronic Health Record Exchange Format and internationally recognized standards (e.g. HL7 FHIR, DICOM, DICOM Web, and IHE profiles), as well as semantic and technical interoperability should be strengthened.
To avoid ambiguity, each data category needs to be further defined for true (structure and semantic) interoperability between EHR-to-EHR and/or EHR-to- medical devices. In particular, when it comes to the medical imaging data category, the requirements need to be further defined as that could be interpreted in different ways by various stakeholders.
2. The governance framework should prioritize standardization needs and improve data interoperability. It should be a natural extension of existing structures, such as the E-health Network and the Multi-Stakeholder Platform (MSP) for ICT standardization, taking into account the reality of the existing global standardization arena. In particular, there should be a link to relevant European and international standards development organizations (SDOs) of all sorts, including industry consortia, and not only to the legally recognized ESOs (CEN, CENELEC, ETSI) or their global equivalents (ISO, IEC, ITU). This must be organized with due stakeholder engagement, in particular with industry. An important goal would be to align on shared views on the need for standards as input for SDOs, who could then base their own priority setting on better and more homogeneous market demand insights.

Article 5.1

*Where data is processed in electronic format, Member States shall **follow international***

data interoperability standards as well as the Commission Recommendation (EU) 2019/243 on a European Electronic

Health Record exchange format to implement

access to and exchange of personal electronic health data for primary use fully or partially falling under the following categories:

(...)

Reimbursement of cross-border telemedicine services

As acknowledged in the EHDS Communication, telemedicine has become an integral part of healthcare during the COVID-19 pandemic and beyond. Bitkom welcomes the Commission's proposal to include provisions for cross-border telemedicine services in the proposal to fully enable patients to benefit from remote consultations, also across borders. Therefore, a compromise should be attempted in the EHDS which could be agreeable by the Member States in the Council to avoid the deletion of Article 8 as a whole.

Article 8

Where a Member State accepts the provision of telemedicine services, it shall~~, under the same conditions, accept~~ support the provision of the services of the same type by healthcare providers located in other Member States, in accordance with national legislation.

Identification management

Article 9.2 should be amended to reflect the dynamic nature of identity management technology. Currently, due to Article 9.1, the identity management is technologically fixed in its current statutory embodiment. This prohibits the further development of State of the Art ID-Management in the context of the EHDS. By amending Article 9 § 2, the regulation becomes more technology agnostic and enables the aforementioned development.

Article 9.2

The Commission shall, by means of implementing acts, determine the requirements for the interoperable, cross-border identification and authentication mechanism for natural persons and health professionals, in accordance with Regulation (EU) No 910/2014 as amended by [COM(2021) 281 final]. The mechanism shall facilitate the transferability of electronic health data in a cross-border context. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in

Article 68(2). ***The Commission shall assess and modify the requirements determined as necessary in order to reflect advances in the technological field of identification and authentication mechanisms. Such assessments shall be performed bi-annually or in shorter intervals as determined by the Commission. The commission shall also align the access to EHDS referring to a uniform EU Digital Identity architecture.***

Digital health authority

It is key that public players define norms and foundation bricks of the digital health sector, filling gaps without altering existing well-functioning markets, to ensure an environment where innovation can thrive. Therefore, we would suggest erasing from the text the call on Member States to offer telemedicine services and the call on Member States to provide through "MyHealth@EU" additional services to facilitate healthcare access and public health purposes. They should rather support the existing offers and promote that such services are easy to use, accessible to different groups of natural persons and health professionals.

Article 10.2

~~*(k) offer, in compliance with national legislation, telemedicine services and ensure that such services are easy to use, accessible to different groups of natural persons and health professionals, including natural persons with disabilities, do not discriminate and offer the possibility of choosing between in person and digital services;*~~

Article 13.1

~~*Member States may provide through MyHealth@EU supplementary services that facilitate telemedicine, mobile health, access by natural persons to their translated health data, exchange or verification of health-related certificates, including vaccination card services supporting public health and public health monitoring or digital health systems, services and interoperable applications, with a view to achieving a high level of trust and security, enhancing continuity of care and ensuring access to safe and high-quality healthcare. The Commission shall, by means of implementing acts, set out the technical aspects of such provision. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 68(2).*~~

Chapter III EHR systems and wellness applications

Interplay with legislation governing medical devices and AI systems

The proposed Article 14, which intends to clarify the interplay with medical devices under MDR and high-risk AI systems proposed in the AI Act, is insufficiently clear. It needs to be clarified to prevent requiring the manufacturer to conduct conformity assessments under all three regulations (MDR, AI Act and EHDS).

Article 14. (2) creates a contradiction with the overall purpose of this regulation. To ensure legal certainty, it is necessary to clarify that any software used in the healthcare environment that falls under the definition of an EHR system shall comply with this chapter (unless such software is already subject to similar regulation i.e. see case of medical devices).

Article 14.2

(...)

~~*This Chapter shall not apply to general software used in a healthcare environment.*~~ ***Manufacturers of EHR systems that also qualify as medical devices as defined in Article 2(1) of Regulation (EU) 2017/745 and claim interoperability of those medical devices with EHR systems under this Regulation shall prove compliance with the essential requirements on interoperability laid down in Section 2 of Annex II of this Regulation. Article 23 of this Chapter shall be applicable to those medical devices.***

(...)

Placing on the market and putting into service

Given that modifications to the EHR system may not necessarily be done by the manufacturer, obligations and responsibilities by any party who makes such changes should be clearly recognized.

*Article 15.**3***

If any economic operator, other than the manufacturer, makes modifications to the EHR system while deploying or using it which lead to changes in the intended purpose and deployments recommendations for the EHR system as declared by the manufacturer, the economic operator shall

assume the responsibilities of a manufacturers under this Regulation for the EHR system's compliance with this Regulation.

In case of any malfunctioning or deterioration in performance quality due to the changes made by the economic operator during deployment or use of the EHR system contrary to the manufacturers 'recommendations for technical deployment of the system or purpose of its use, full responsibility for those modifications lays with the economic operator.

Common specifications

Internationally, consensus standards should be the preferred means to demonstrate conformity with essential requirements set out in Annex II of this Regulation. Common specifications should only be developed as the last resort because their development lacks transparency and does not allow for proper consultation with stakeholders. Common specifications take a long time to be developed and can rarely be considered as state-of-the-art necessary for ensuring security. Security in the context of health

data spaces shall be the overriding goal, and thus standards shall be preferred over common specifications. The necessary amendments shall also be reflected in para. 4-6 of this Article.

Article 23.1

Where harmonized standards do not exist and are not expected to be published within a reasonable period or where the Commission considers that the relevant harmonized standards are insufficient or that there is a need to address specific interoperability concerns, *the Commission* ~~*shall*~~ *may, by means of implementing acts* ***and only after consulting the European standardization organizations as well as the relevant stakeholders*** *adopt common specifications in respect of the essential requirements set out in Annex II, including a time limit for implementing those common specifications.* ***The Commission should duly justify why it has decided not to request the development of harmonized standards.***

Where relevant, the common specifications shall take into account the specificities ***and verify compatibility with sectorial legislation and harmonized standards, like the Medical Device Regulation,*** *of medical devices and high-risk AI systems referred to in paragraphs 3 and 4 of Article 14*~~*,*~~ ***including the state-of-the-art standards for health***

informatics and the European electronic health record exchange format*. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 68(2).*

Chapter IV: Secondary use of electronic health data

Obligations to share health data

The obligations for sharing health data are too broad. They include processed data from the research context, often generated with considerable private-sector resources. These far-reaching obligations are not matched by sufficient guarantees for the protection of intellectual property and trade secrets. The mere risk of obligations to disclose trade secrets could prevent companies from collecting certain data in the first place – with potentially far-reaching consequences for data-driven innovations in healthcare. We therefore propose to integrate an explicit right of objection for corresponding, business sensitive data categories.

Article 33.1

Data holders shall make the following categories of electronic data available for secondary use in accordance with the provisions of this Chapter ***with the right to refuse access to their data if:***

a) it compromises the scientific integrity of a scientific research study, including a clinical trial;

b) it compromises the protection of data entailing IP rights, trade secrets or commercial property;

To create trust in the exchange and handling of business-sensitive data and thus to avoid the negative effects for individuals mentioned before, generally applicable terms of use should be developed. These should include the following points in relation to confidential data:

- Obligation of confidentiality
- Data users shall ensure trade secrets and other confidential data like IP rights retain this status after provision, also by providing technical measures

- Data users shall ensure not to infringe or misappropriate the data holders IP rights, trade secrets or commercial property
- Data users shall use the data received solely to the extent required for conducting the secondary use agreed on with the data holder.
- The data holder should own any derived form of its shared data ('derived data') that is created by the user.
- Sanction mechanisms for violation of the terms of use

Minimum categories of electronic data for secondary use

Given the type of data included in Art 33 Clause 1, it should be clarified that the Clause covers health-related data.
It is proposed to delete sub-clause (k) because relevant health data, processed by medical devices must be included in the EHR and inclusion of data from medical devices may impose additional technical requirements for medical devices and confusion in regards of who is the data holder under the EHDS.

The list of the minimum categories of electronic health data for secondary use should also include laboratory data which are crucial in the diagnosis and treatment of diseases as well in providing insights into how to improve outcomes at the population level.

Article 33.1

*Data holders shall make the following categories of electronic **health** data available for secondary use in accordance with the provisions of this Chapter:*

(...)

*(m) electronic health data from **laboratories,** biobanks and dedicated databases;*

Unless the proposed adjustment is introduced, this clause implies that even without emergency circumstances IP and trade secrets data must become open under the excuse of secondary data use, which carries high risk of creating a lot of damage to the incentives to innovate in the EU with no clear benefits for the EU citizens and the economies.

Article 34.2

Electronic health data entailing protected intellectual property and trade secrets from private enterprises shall be made available for secondary use when the purpose of the use meets the criteria of exceptional need as defined under 'public emergency' situations in the Data Act Regulation [...], which cannot be otherwise addressed. Where such data is made available for secondary use, all measures necessary to preserve the confidentiality of IP rights and trade secrets shall be taken.

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

Secondary use of electronic health data for development and innovation activities for products and services in Article 34.1 (f) should be broader and include those products and services that contribute to health, care and well-being of natural persons, as well as to the general interest of the society as intended by the proposal.

Article 34.1

Health data access bodies shall only provide access to electronic health data referred to in Article 33 where the intended purpose of processing pursued by the applicant complies with:

(...)

*(f) development and innovation activities for products or services contributing to public health, **care and well-being** or social security, or ensuring high levels of quality and safety of health care, of medicinal products or of medical devices;*

*(g) training, testing and evaluating of algorithms, including in medical devices, AI systems and digital health applications, contributing to the ~~public~~ health, **care and well-being** or social security, or ensuring high levels of quality and safety of health care, of medicinal products or of medical devices*

Tasks of health data access bodies

Industry representatives carry important technological and digital health related products and services' deployment competencies. Therefore, they should be included to ensure efficient fulfilment of the tasks, prescribed to health data access bodies in clause 1 of article 37.
Similarly, the term "industry" should be added to Articles 65 (1) e and (2) f.

Article 37.2

In the exercise of their tasks, health data access bodies shall:

(...)

*(c) cooperate with stakeholders, including patient organizations, representatives from natural persons, health professionals, **industry**, researchers, and ethical committees, where applicable in accordance with Union and national law;*

Fees

The cost of data extraction, anonymization and making it available should be included. Also, it will be difficult for data holders to set up personalized fees for SMEs, public bodies, Union institutions, bodies, offices and agencies involved in research, health policy or analysis, educational institutions and healthcare providers depending on their size and budget. It may be more feasible to establish certain criteria based deductions for data provision fees for the mentioned list in case it pursues specific interests of the society which are perceived as high priority and have specific needs yet are capable to complete the research or product development in a quality way for which the data is requested.

Article 42

1. *Health data access bodies and single data holders may charge fees for making electronic health data available for secondary use. Any fees shall include and be derived from the costs related to conducting the procedure for requests, including for assessing a data application or a data request, granting, refusing or amending a data permit pursuant to Articles 45 and 46 or providing an answer to a data request pursuant to Article 47, in accordance with Article 6 of Regulation [...] [Data Governance Act COM/2020/767 final] **including the***

technical and operational costs to extract the data and to make them available.

2. *Where the data in question are not held by the data access body or a public sector body, the fees may also include compensation for part of the costs for collecting the electronic health data specifically under this Regulation* ***and the costs of the technological investments to extract and make the data available and to anonymize them /pseudonymize them.*** ~~*I*~~*In addition to the fees that may be charged pursuant to paragraph 1. The part of the fees linked to the data holder's costs shall be paid to the data holder.*

(...)

3. *Any fees charged to data users pursuant to this Article by the health data access bodies or data holders shall be transparent and proportionate to the cost of collecting and making electronic health data available for secondary use, objectively justified and shall not restrict competition. The support received by the data holder from donations, public national or Union funds, to set up, develop or update tat dataset shall be excluded from this calculation. The specific interests and needs of SMEs, public bodies, Union institutions, bodies, offices and agencies involved in research, health policy or analysis, educational institutions and healthcare providers shall be taken into account when setting the fees, by reducing those fees* ~~*proportionately to their size or budget*~~ ***according to the predefined percentage of deduction based on the importance of the research to the society and the level of sensitivity of data requested and thus implied technical obligations to ensure maximum personal data protection. In case of data provision at the reduced fee, data recipient must be able to prove that it has sufficient resources, human, infrastructure and capital to complete the research and/or product development for which data is requested and that the use of data will comply with provisions under this Regulation and the Data Act.***

Data sharing timeframe

Such formulation in principle leaves discretion for undefined delays in data provision as long as formal procedures are followed. Reasonable grounds condition should be introduced to ensure efficient functioning of the public authorities under this Regulation.

Article 46.4

Following the issuance of the data permit, the health data access body shall immediately request the electronic health data from the data holder. The health data access body shall make available the electronic health data to the data user within 2 months after receiving them from the data holders~~, unless the health data access body specifies that it will provide the data within a longer specified timeframe~~.

Additional point for single data holder: The timeframes for HDABs and single data holders to provide a decision on data access requests (2 months with a possible 2 month extension under Article 41) are too short and do not consider the high burden of data collection.
In Article 49(2), to amend the wording to the (single) “data holder may decide to follow the procedures in” Article 46 and Article 47. Article 49(2) currently states that a “single data holder” may issue a permit, in accordance with Articles 46 (and 47). These provisions then state that “if the requirements in this Chapter are fulfilled by the applicant… …[the entity performing the review] shall issue a data permit”. Due to the discretion inherent to the permitting procedure, the word “may” by itself is not sufficiently clear.
Need to clarify whether the data holders would have the right to use the HDAB’s secure processing environment to avoid single data holders deciding to follow EHDS procedures having to develop their own or having to enter into costly contracts. In cases where the data holder is a single data holder, the provisions in Article 49 could be interpreted as requiring them to act as a de facto HDAB, providing data through a “secure processing environment” and reporting to the national access body on a continuous basis (3 months after permitting or approving). This is bound to result in a disproportionate burden on these data holders, and the assumption is that this is unintentional.

On data permits: need for harmonized set of rules to assess the application for data access or data request in order to ensure the uniform implementation and interpretation of EHDS across the EU. The criteria for assessment and decision-making need to be further clarified, including criteria which may delay application or lead to refusal. To avoid building 27 different data space regimes, all HDABs should use common templates and harmonized approaches for evaluating data access requests, adding specific criteria for them to consider and justify decisions concerning requests and permits (cf. Articles 36 and 37).

The idea of the 'secure processing environment' (SPE) is a step in the right direction but needs to be further elucidated. For example, clarity is needed on whether data users can bring their own analytic tools and algorithms to the environment to maximise the insights from the data.
Additionally, the current default option to grant the permit is clearly a less appropriate option to incentivize health data access bodies' decision-making than, for example, investment in human and other operational resources. The same can be said of the derogation from permit requirements for public bodies.

Anonymisation and pseudonymisation

The inclusion of pseudonymised data in scope for sharing is welcome as it can often provide invaluable clinical insights that cannot possibly be achieved using anonymised data, but a consistent interpretation of anonymisation and pseudonymisation will be essential to harmonise rules across the bloc.
There is a need for approvals for secondary use of health data to be consistent and harmonised across Europe. Legal and ethical criteria for approving pseudonymised data use and data linkage need to be more formally specified at a European level to encourage a more harmonised and consistent approach. Furthermore, a conservative interpretation of anonymisation would have limited data utility for R&D and healthcare delivery, considering some research activities are likely not possible with anonymous data, such as research involving genetic data where anonymisation would be difficult. Co-legislators and other relevant authorities should also consider the inherent privacy offered by federated data networks in the secure processing environment set out in the EHDS proposal. A federated approach allows for architectural privacy enhancing technologies, such as federated learning and multiparty computation, which are considered as very robust. Other, often complementary, privacy-enhancing technologies should also remain an option as the field develops, that may involve adding noise, performing calculations on encrypted data, or synthesising data. The point being here that different use cases require different technologies, and the personal/non-personal dichotomy does not necessarily allow for the most optimal (or even most secure) approach.

Recommendation: In line with the principle of GDPR under Recital 26 on "all the means reasonably likely to be used" to re-identify someone, we should shift our understanding from 'anonymisation' as an absolute term to 'relative anonymisation'. We therefore advocate for the recognition of relative anonymisation methodology, which takes into account relevant factors such as the type of use and the controls in place and reduces this probability of re-identification to a sufficiently low level. No prescriptive anonymisation methodology should be imposed because different approaches will be required depending on the intended research use. Any ethical approvals required to access pseudonymised data should be more clearly spelled out, as these would go beyond the standard data protection impact assessments (cf. Article 45(4)).
When properly justified, data linkage should be allowed in order to make treatment development faster (e.g. critical for rare disease patients).

The proposal should state whether HDABs or data holders will be responsible for data anonymisation or pseudonymisation. Should the data holder be responsible, they should be allowed to charge for the service at fair market value.

European Health Data Space Board (EHDS Board): Composition and monitoring duties
Bitkom welcomes the legislator's intention to establish an EHDS board. Involvement in the Board for all stakeholders, including industry, should be ensured to leverage expertise and lessons learnt by all stakeholders that are working to establish an optimal data and digital ecosystem (cf. Article 64(4)). Similar to the Data Governance Act's Data Innovation Board, the EHDS might specify which stakeholders will be involved in what way in its sub-groups.This is the only way to ensure an implementation in line with patient needs and within an ambitious and realistic framework.

Furthermore, the importance of a uniform implementation of the secure processing environment across all member states should be considered. Such monitoring has already been used in the former legislation (cf. Art. 70, GDPR). Its composition and cross-sectoral expertise pointed out above, make it possible to rely on the EHDS Board for this task.

Article 50.4

The Commission shall, by means of implementing acts, provide for the technical, information security and interoperability requirements for the secure processing environments. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 68(2). ***The EHDS Board shall ensure the consistent implementation of the secure processing environment across Member States while ensuring compliance with the technical, information security and interoperability requirements provided by the Commission.***

Authorized participants of HealthData@EU

Industry should be included as the authorized participant of HealthData@EU, because it produces important input into R&D and technological innovation.

Article 52.3

Union institutions, bodies, offices and agencies, ***as well as private legal entities*** *involved in research, health policy or analysis, shall be authorised participants of HealthData@EU.*

Chapter V: Additional actions

Third country transfer of non-personal electronic data

Data streams are global. A free flow of data, especially transatlantic, is of outmost importance for Europe as a business and innovation location. The proposed international data access and transfer requirements risk imposing data localization and may result in non-EU jurisdictions implementing as a counter-reaction data localization as well, which would increase data fragmentation. Against this background, Articles 61 et seq. of the draft regulation require a fundamental revision.

This applies first to **Article 61**, which contains complex rules on the transfer of non-personal data to third countries (para. 1). It builds explicitly on the Data Governance Act's protective regime for 'highly sensitive data categories of non-personal data'. This goes beyond the definition of 'data concerning health' established by the GDPR. The provision should be deleted or at least added in such a way that the safeguards to be established by the delegated act (para. 2) allow international data transfers for science and research.

> *Article 61*
>
> 4. *Non-personal electronic **health** data made available by health data access bodies, that are based on a natural person's electronic **health** data falling within one of the categories of Article 33 [(a), (e),] shall be deemed highly sensitive within the meaning of Article 5(13) of Regulation [...] [Data Governance Act COM/2020/767 final], provided that their transfer to third countries presents **an objective** risk of re-identification ~~through means going beyond those likely reasonably to be used~~, in view of the limited number of natural persons involved in that data, ~~the fact that they are geographically scattered or the technological developments expected in the near future~~.*
> 5. *The protective measures for the categories of data mentioned in paragraph 1 shall ~~depend~~ **take into account** ~~on~~ the nature of the data and anonymization techniques and shall be detailed in the Delegated Act under the empowerment set out in Article 5(13) of Regulation [...] [Data Governance Act COM/2020/767 final].*

Article 62 provides additional general requirements to prevent international transfer or governmental access to non-personal electronic health data held in the European Economic Area. However, Article 63, by noting that for international transfers and access of personal electronic health data "Member States may maintain or introduce

further conditions, including limitations", contradicts the objective of the proposal to "harmonise data flows to support natural persons in benefiting from protection and free movement of electronic health data", both intra-EU, as well as with trusted countries, and risks to further exacerbate the existing fragmentation.

It should be noted that, as it stands, while pseudonymised electronic health data can be used when in a secure processing environment (SPE), should the data be downloaded from the SPE, it can only be in non-personal form (Art 50(2)). As a result, any transfers from data holder to data user (permitted by a health data access body) would contain exclusively non-personal electronic health data. When data is shared for use in pseudonymised format, this would happen only within the SPE. In primary use, electronic health data is to remain in the health or social security sector. In other words, for better or worse, we do not expect a sudden and uncontrollable flow of personal electronic health data originating from the EHDS.

We would recommend in the context of the EHDS to remove the proposed additional restrictions related to access to and transfer of non-personal data outside the EU since personal data in scope of EHDS is already covered by GDPR, incl. wrt its international transfer, as well as by DGA when it comes to sensitive data sets. Other data sets would concern non-personal data and therefore do not necessitate additional protection. We also caution against enabling more fragmentation, cf. Art. 63 – which would be contradictory to the EHDS objectives at harmonisation of health data use.

Penalties

Clear rules shall be set for penalties applicable to infringements to ensure harmonized deployment and safeguard mechanisms across the Member States. It could follow similar principles as established under the GDPR.

Article 69

1. *Member States shall lay down the rules on penalties applicable to infringements of this Regulation and shall take all measures necessary to ensure that they are implemented. The penalties shall be effective, proportionate and dissuasive. Member States shall notify the Commission of those rules and measures by date of application of this Regulation and shall notify the Commission without delay of any subsequent amendment affecting them.*

2. ***Penalties shall cover infringements not addressed by the MDR/IVDR and GDPR and shall depend on the circumstances of each individual case. When deciding whether to impose a penalty and deciding on the***

amount of the penalty in each individual case due regard shall be given to the following:

(a) the nature, gravity and duration of the infringement taking into account the nature scope and level of the damage done.

(b) the intentional or negligent character of the infringement.

(c) any action taken by the EHR provider, deployer or data holder to mitigate the damage of the infringement.

(d) the degree of responsibility by the responsible for the infringement party taking into account technical and organisational measures implemented to prevent the infringement.

(e) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement.

(f) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

3. *If the EHR system provider or data holder intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the penalty shall not exceed the amount specified for the gravest infringement.*
4. *Infringements of the following provisions shall be subject to penalties of up to 2 000 000 EUR, or up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.*
5. *The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.*
6. *Where the legal system of the Member State does not provide for penalties, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those*

legal remedies are effective and have an equivalent effect to the penalties imposed by supervisory authorities.