DIGITALEUROPE

19 JANUARY 2023

DIGITALEUROPE's Position Paper on the European Health Data Space proposal

Executive summary

DIGITALEUROPE welcomes the European Commission's proposal for a Regulation on the European Health Data Space (EHDS), and strongly supports its objectives. The EHDS can create important harmonisation by establishing well-governed access to health data for the delivery of healthcare services, and by regulating a wide range of secondary use purposes to support better health outcomes. This could increase Europe's capability and global competitiveness in health research and innovation, and strengthen its health systems and public health resilience.

In this paper, DIGITALEUROPE provides recommendations on possible improvements to the EHDS proposal, which correspond to challenges identified by a diverse set group of stakeholders, such as:

- The need for alignment with all relevant horizontal and sectoral European legislation, including the General Data Protection Regulation (GDPR), the Medical Devices Regulation (MDR), the AI Act and the Cyber Resilience Act. Confusion needs to be avoided with critical definitions enshrined in the GDPR, the Data Governance Act or (proposed in) the Data Act.
- The need to clarify the scope of the rights of natural persons in relation to the primary use of their electronic health data and the relation of these rights with corresponding rights under the GDPR and the Data Act.
- The need to set forth clearly the definition of an 'electronic health record (EHR) (system)' to avoid covering all products and services interacting with electronic health data at any point.
- The need to advance a digital single market for telemedicine services.
- The need to clarify the general conditions and the governance and mechanisms for secondary use of electronic health data.

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

- The need for alignment with the Trade Secrets Directive (TSD) and protection of trade secrets and intellectual property (IP) rights.
- The need to provide clarity and harmonised processes for health data access bodies by specifying requirements for data holders and data users. There is also a need to describe more clearly what is the criteria that may delay a data permit application or lead to refusal, and how specific minimum categories of electronic health data are intended to be included.
- The need to remove the proposed additional restrictions relating to international access to and transfers of non-personal data in the context of the EHDS.
- The need to avoid bottlenecks by permitting successful data sharing to continue through voluntary bilateral and multilateral agreements, which are not necessarily channelled through the EHDS.
- The need for the European Health Data Space Board to involve all stakeholders including industry representatives to leverage expertise.

The EHDS could enhance the quality of healthcare and medical innovation in Europe, and unleash much-needed investment, if policymakers can ensure regulatory alignment and consistency without eroding established legal rights and concepts. However, we caution that the EHDS by itself cannot address all data-related regulatory challenges in healthcare. The fragmentation across the EU in the interpretation and application of the GDPR, both for primary and secondary use of health data, continues to hamper research and innovation in Europe.

Table of contents

Introduction

DIGITALEUROPE, in a consensus statement with a group of 35 stakeholders, including medical professional and research organisations, patient representatives, industry associations and existing data collaborations, welcomes the European Commission's proposal for a Regulation on the European Health Data Space (EHDS). Together, we strongly support its objectives.

DIGITALEUROPE believes the adoption of the new legislation can bring important European harmonisation and rapidly scale up well-governed access to health data for the delivery of healthcare services, and support a wide range of secondary use purposes for better health outcomes. This could increase Europe's capability and global competitiveness in health research and innovation, and strengthen its health systems and public health resilience.

We emphasise the need for alignment with all relevant horizontal and sectoral European legislative acts. The regulatory framework could become an enabler for innovation in Europe, if it ensures regulatory alignments, consistency and certainty, attracts much-needed investment, and does not erode established legal rights and concepts.. The proposal should clarify ambiguous definitions and establish proportionate requirements that are aligned with existing and future EU legislation, as well as international consensus standards, and where necessary, define clear rules for their order of precedence and prevalence.

DIGITALEUROPE's Executive Council for Health has released two reports providing a vision for industry's role in digital transformation. The first is a report on the building blocks for a trustworthy EHDS and use cases, which highlights, for instance, the need for a "single access point" for the secondary use of health data, central health data bodies supported by an EU-level entity, easy to use eID services, and a simple common consent form for cases when consent is required.

The second report focuses on the potential and needs for health innovation to be driven in Europe identifying 10 areas where Europe can enhance innovation in healthcare, including: personalised care plans, preventative care, integrated care, digitalisation of surgery, remote consultation monitoring and care, innovation and decentralisation of clinical trials and investigation, precision medicine, and advanced models and digital twins.

DIGITALEUROPE represents a uniquely wide range of companies across the spectrum from pure technology to more traditional healthcare companies, as well as national trade association members. In this paper, we elaborate in more detail on the digital industry's recommendations for the EHDS.

Overarching provisions

Above all, this proposal is intended to harmonise and clarify health data rules and governance across Europe. Health communities and innovators cannot afford further uncertainty and fragmentation in Europe, which would undermine the adoption of digital health technologies.[1]

Therefore, there should be a clear hierarchy between the EHDS proposal and other existing or proposed EU legal acts, as well as clarity about its relation with national legislation, to avoid confusion and duplications. As it stands, the proposal leaves too much room for Member States to provide further rules on several aspects, such as individuals' rights to restrict access to their data or health professionals' access to electronic personal data, but also regarding requirements for secondary use,[2] that it is not fully clear what the impact would be on the industry.

This is further complicated with the concurrent negotiations on horizontal proposals, which would impact the EHDS, because they will regulate commercial and industrial data, processing services, AI products and services, and products with digital elements.[3] Not only is there a newly established definition for 'electronic health data' and 'electronic health record system' that raise concerns. There are also several definitions set forth by the EHDS proposal that appear inconsistent with definitions in other existing or proposed legislations, most notably the notions of 'data holder', 'data recipient', and 'data user.' This needs to be clarified and aligned.

Clarity in this regard is key, not least because the scope of obligations and requirements are delineated based on the cumulative requirement that the data in question concerns 'electronic health data' and that the 'data holder' is an "entity or a body in the health or care sector, or performing research in relation to these sectors" (cf. Art 2(2)(y)), while under Chapter II, Article 3, both the 'data holder' and the 'data recipient' should be "from the health or social security sector" and under Chapter IV the 'data user' is not limited to a specific sector.

Finally, but crucially, there remains an undiminished need for a fully harmonised interpretation and application of the GDPR across the EU for both primary and secondary use of health data. Major issues remain unresolved, such as the lack of common interpretation of the concept of 'non-personal data',

[1] The Assessment of the EU Member States' rules on health data in the light of GDPR, commissioned by the DG Health and Food Safety, found that the application of the GDPR's rules relating to the processing of health data is highly fragmented across EU Member States.

[2] Notably, for primary use under Arts. 3(3), 3(5), 3(9), 4(2), 4(4); for EHR systems under Art. 14(5); for secondary use under Article 45(4), and on international transfers and access under Art. 63 . It should also be noted that specific rules for primary use (such as on restriction of access or obtainment of information) can significantly impact the operationalisation of secondary use.

[3] The Data Act (COM/2022/68 final), the AI Act (COM/2021/206), and the Cyber Resilience Act (COM/2022/454).

sufficient anonymisation and pseudonymisation (cf. Rec. 43), divergent application of the appropriate legal basis for secondary use, and harmonised rules for international data transfers of personal data (cf. Art. 63).

Many of these issues could be addressed under Chapter I on General provisions that sets out the scope of application and the relationship with other legal acts (and definitions).

Chapter I – General provisions

Subject matter and scope (Art. 1)

Article 1 lays down the objectives of the Regulation and the entities which would fall under the scope of all or some of its provisions, as well as its relationship with other legislation. DIGITALEUROPE believes some improvements are needed, especially to avoid confusion regarding their interaction with fundamental rights and intellectual property (IP) rights.

Recital 5 clarifies that electronic health data covers personal data as defined in the GDPR and non-personal data, and that "[t]he electronic health data [in all Chapters] *concern all categories of those data*… …and *should also include inferred and derived data*, such as diagnostics, tests and medical examinations, as well as *data observed and recorded by automatic means*" (emphasis added).

DIGITALEUROPE recommends:

- In order to align with the GDPR, Article 1(3)(b) should be amended to read as follows: "This Regulation applies to: […] (b) controllers and processors established in the Union processing *personal* electronic health data of Union citizens and third-country nationals legally residing in the territories of Member States".
- For further consistency, another point could be added under Article 1(3) specifying that the Regulation also applies to "data holders as defined in this regulation when the relevant provisions concern *non-personal* electronic health data."
- Additionally, Article1(3)(d) should add 'data recipients' to read "*data recipients and* data users to whom electronic health data are made available by data holders in the Union."
- For consistency with provisions for the protection of trade secrets, Article 1 should include an explicit reference to the Directive on the Protection of Trade Secrets (Directive (EU) 2016/943), which should take precedence. If not, this might also contravene the EU's and Member States' obligations under the WTO Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) (see Council

Decision 94/800/EC). For example, as a result of the proposed EHDS regulation and its effects, none of the conditions for what constitutes 'trade secret' according to Article 2(1) of Directive (EU) 2016/943 should be considered as no longer applying.

Definition of 'data holder' (Art. 2(2)(y))

The current definition borrows language from definitions of 'data holder' under the Data Governance Act and the Data Act, and adds certain elements to them. As a result, it inherits problems present in both legislative instruments, especially in the latter, which may lead to further complexity. There is also misalignment with the concepts of 'controller' and 'processor' under the GDPR. As this crucial definition is unclear, this may hinder consistent interpretation by policymakers, courts, data providers and data users – in case of both personal and non-personal electronic health data.[4]

DIGITALEUROPE recommends:

To improve alignment within the EHDS and with other data-related legislation, the definition should clarify that an entity may qualify as a 'data holder' in three processing scenarios. Accordingly, a 'data holder' should be an entity:

- which acts as a controller under the GDPR[5] regarding the processing of personal electronic health data for primary use, and/or
- which has an obligation under the Regulation, other Union law or national legislation implementing Union law to make electronic health data available for secondary use, and/or
- which, in the case of non-personal electronic health data, controls and has the ability to make data generated by a medical device, wellness application, EHR system or related services available.

⏩ This could be further elaborated to fit the specific context of the EHDS. Context-specific clarifications could include, for example, that in the case of a clinical trial, the clinical trial sponsor (or EU legal representative, if the sponsor is not in the EU) would be the data holder for clinical trial data.

Chapter V – Additional actions

International data access and transfers

The proposed international data access and transfer requirements risk imposing data localisation and may result in non-EU jurisdictions implementing

[4] Further clarity on the scope can be found in Art. 1(3)(b): "controllers and processors established in the Union processing electronic health data of Union citizens and third-country nationals legally residing in the territories of Member States;".

[5] Under Article 4(7) GDPR 2016/679.

as a counter-reaction data localisation as well, which would increase data fragmentation.

Article 61 builds explicitly on the Data Governance Act's protective measures for 'highly sensitive data categories of non-personal data' to be further specified in a delegated act. The provision lists specific health data categories from which derived non-personal data would still be considered 'highly sensitive', if "their transfer to third countries presents a risk of re-identification through means going beyond those likely reasonably to be used".[6] This interpretation goes beyond the definition of 'data concerning health' established by the GDPR.

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.

Finally, 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.

DIGITALEUROPE recommends:

- A well-coordinated approach to achieve consistency between data-related initiatives under the Data Strategy. Although they aim to regulate transfers of non-personal data, the Data Governance Act, the Data Act and Chapters IV and V of the EHDS address laws that tend to involve personal data and are already covered by the GDPR. Therefore, in the context of the EHDS, the EP and the Council should remove the proposed additional restrictions related to access to and transfer of non-personal data outside the EU.

[6] They are the following categories: (a) EHRs, (e) human genetic, genomic and proteomic data, (f) person generated electronic health data, including medical devices, wellness applications or other digital health applications, (i) electronic health data from medical registries for specific diseases, (j) electronic health data from clinical trials, (k) electronic health data from medical devices and from registries for medicinal products and medical devices, (m) electronic health data from biobanks and dedicated databases.

- To consider critically whether the addition of Article 63 on personal electronic health data fulfils a material purpose in the operational part of the EHDS, and whether that outweighs the potential for confusion and legal uncertainty (i.e. by *a contrario* reasoning, where other relevant GDPR aspects are not mentioned explicitly, what could lead to interpretations that the EHDS deviates from and/or supersedes the GDPR).

As is described concretely in DIGITALEUROPE's report on Transfers in the data strategy: Understanding myth and reality, the Data Strategy overlooks the substantive protections that Europe has already created for personal data, and is bound to generate conflicting interpretations and enforcement, and lead to overregulation of data. If the EU gets the regulation wrong, then this could jeopardise the crucial international dimension of robust health research.

Primary use of electronic health data

Chapter II does not duly consider the interaction of the EHDS with existing and proposed legislation, particularly the GDPR and the proposed Data Act. On a general note, finding a good fit and clear alignment would support the formulation and operationalisation of core definitions. Clarity in this regard would help different stakeholders, including those acting as controllers or processors (in the meaning of the GDPR) to meet their obligations and duties when it comes to electronic health data.

Rights of natural persons (Art. 3)

Article 3 sets out specific provisions concerning the rights of natural persons in relation to the processing of their personal data in the context of healthcare, for example to have access to their personal electronic health data, immediately, free of charge and in an easily readable, consolidated and accessible form. Patients' access to and control over their health data can have great benefits in, among others, understanding their state of health and managing their health, including adherence to prescribed therapies.

The proposal aims to build on the "right of access to data by a natural person, established by Article 15 of [the GDPR]… …in the health sector" (Recital 8), for instance, by making this more immediate and digital, while providing for healthcare-specific exceptions, such as "delaying the display of the concerned personal electronic health data" "where this exception constitutes a necessary and proportionate measure in a democratic society" (Rec 9). The EHDS is the appropriate framework in which to regulate these rights and related obligations and legitimate restrictions. However, the realisation of this would require better alignment with the GDPR and the Data Act, and clarity in terms of their scope.

The scope of these provisions seems ambiguous. For example, they include two exceptions that provide for rights that are not *explicitly* limited to the list of priority categories under Article 5. Generally, for the EHDS to achieve its ambitions, a balance needs to be struck between these rights, the potential layer of additional data governance requirements, and patients' safety. By limiting this to the priorities more clearly, the EHDS would become more manageable for all stakeholders.

DIGITALEUROPE recommends:

- To ensure which categories of data are shared with patients, carers or third parties for the provision and delivery of healthcare by clarifying the relationship between Articles 3 and 5.
- This can be done by adding to Article 3(1) that "[n]atural persons shall have the right to access ~~their~~ personal electronic health data *of the priority categories in Article 5(1) concerning them* processed in the context of primary use of electronic health data, ~~immediately~~ *in a timely manner*, free of charge and in an easily readable, consolidated and accessible form.
- Additionally, in Article 8(3), it should be added that "[n]atural persons shall have the right to give access to or request a data holder from the health or social security sector to transmit ~~their~~ electronic health data *listed in the priority categories in Article 5(1) concerning them* to a data recipient of their choice from the health or social security sector…".
- Ensuring data shared with the patient is meaningful to them. Giving patients access to *all* such data collected on them would not necessarily allow them to derive meaningful insights and could overwhelm them, leading to possible misinterpretations and potential dangers to their health.

Electronic health data access services (Art 3.5)

Article 3(5) sets out provisions for Member States to establish electronic health data access services for the purpose of sharing electronic health data with natural persons.

We urge an approach that does not place disproportionate burden on manufacturers. For example, companies fulfilling data requests, no matter their size, would have to set aside or acquire additional resources from their side to realise the development of structures allowing authentication of such requests and identifying the individual's data among the data sets on the server. Such investments would be disproportionate in the vast majority, if not in all cases. We did not identify substantial evidence in the Impact Assessment (or

elsewhere) for an approach that is at the same time this far-reaching and seemingly indiscriminate.

DIGITALEUROPE recommends:

- In setting up procedures for fulfilling natural person's requests for data, Member States should ensure there is no excessive fragmentation of the process, for instance through guidelines. Fundamentally, it is important that the request for data will not have to be processed by manufacturers holding health data as processors.

Telemedicine, digital health and the Digital Single Market

The COVID-19 pandemic has accelerated the adoption of digital health technologies. Telehealth and remote patient monitoring turned from a novelty into a necessity. Faced with an acute scarcity of resources, healthcare leaders also saw an urgent need to improve data sharing and care collaboration. It would be regrettable to lose the momentum that we have gained in making telemedicine services part of both national and cross-border health care offerings. The uptake of the reimbursement rules should be further supported and aligned across Member States to achieve the Commission's objective of establishing a true EU single market for digital health products and services.

While respecting national competence within healthcare, the EU can still make improvements by facilitating a true single market for digital healthcare services that will make Europe a centre for health innovation.

DIGITALEUROPE welcomes the explicit recognition of the value of digital health and telehealth within the Explanatory Memorandum and the reference under Recital 21 that differences in reimbursement policies should not constitute barriers to free movement of digital health services, such as telemedicine.

In order to foster a single market for digital health services, which, in turn, will support the objective of unleashing the health data economy, several policy options should be considered.

We highlight the priorities:

- Decrease barriers to reimbursement for digital treatment. Reimbursement should focus on treatment/outcomes and not the format it takes.
- Remove limitations on how much of physician and healthcare professional time can be spent on telehealth.
- Remove requirements that patients be tied to a physical centre for their primary healthcare.

DIGITALEUROPE recommends:

- To expand Article 8 to reflect the need for common and specific measures that Member States can agree on to reduce fragmentation and the provision and delivery of digital healthcare services.
- To strengthen the support for the provision of digital health services, as set out in Article 8, with stronger binding language within the Regulation, and explicit inclusion of telemedicine services in implementing legislation.
- To clarify in Article 10 that the EHDS-Board shall support digital health authorities in creating joined up telemedicine strategies to ensure that digital services can play a central role in realising European citizens' right to access care across EU borders as provided for in Directive 2011/24/EC.

EHR systems and wellness apps

By providing a definition of what is an 'electronic health record' and 'EHR-system', the Regulation essentially creates a European baseline for what should be a digital version of a patient's health record, potentially creating a harmonised market for a rapidly developing field of innovation. The same could be said for 'wellbeing applications' and their labelling scheme.

To regulate these EHR-systems, Chapter III provides a self-certification framework coupled with essential requirements. Article 14(1) then aims to delineate the scope of the Chapter III to those "intended by their manufacturer for primary use of priority categories of electronic health data referred to in Article 5"

Overall, Chapter III brings yet another dimension of complexity for companies and users to consider when exploring, developing and bringing to the market their innovations. These concerns were strongly emphasised in the aforementioned consensus statement signed by 35 stakeholders including DIGITALEUROPE.

We strongly suggest that improvements are made to avoid disproportionate, overlapping or contradictory regulations, but also to agree at European level on an accurate definition of EHR (systems) that clearly defines the limiting characteristics of what constitutes as such.

EHR systems, medical devices and AI

Manufacturers of EHR systems and potential users of EHR data may appreciate the holistic approach of the proposal to improve the availability, quality and interoperability of electronic health data from the data source and

throughout the lifecycle of data use. However, this will not inevitably facilitate innovation, when compliance risks are high due to legal uncertainties.

The choice for self-certification shows the need for a proportionate approach, further evidenced by the Impact Assessment[7], which indicates that there has been a substantial move away from third-party conformity assessment. Harmonisation can be achieved through Chapter III in conjunction with Annex II, which aim to regulate general elements, such as intended performance, but primarily regulate interoperability and security (16 out of 18 essential requirements concern these two aspects).

Even with a self-certification mechanism, some major issues must be addressed: notably the definition of EHR systems, clarifying the notion of "intended purpose" and delineating EHR systems from other products and services "claiming interoperability", and simplifying compliance and interplay.

Honing the scope for compliance

Under Article 2(2)(n), the EHDS proposal defines 'EHR systems' as "any appliance or software intended by the manufacturer to be used for storing, intermediating, importing, exporting, converting, editing or viewing electronic health records".

This definition could concern any type of software, for example: software which is simply meant to generate and process this information before their inclusion in the general patient record or software embedded in an MRI (a ubiquitous imaging scan). Similarly, the 'Electronic Health Record' definition also does not refer to some of the key aspects of what constitutes an EHR in practice.

As a general principle, the better the scope is delineated and focused only on HER systems that are intended as such and consolidate and retain health-related data, the more proportionate any essential requirements and conformity assessments would be. There are several reasons why the current definition of scope is bound to lead to unintended consequences.

Firstly, the current perimeter of Chapter III could lead to broad interpretations. It intends to set out the rules for placing on the market, and putting into service, products or services "intended as" EHR systems for primary use of priority categories, and those "claiming interoperability" with them, without further clarification. Theoretically, due to currently ambiguous constructions, even if a medical device would not claim interoperability with EHR systems, but would fall within the definition of an EHR, the EHDS would still apply. Similarly, this also holds true for medical devices intended to provide data for the EHR and EHR systems.

[7] Impact Assessment on the European Health Data Space (May 2022), available at https://health.ec.europa.eu/publications/impact-assessment-european-health-data-space_en

Secondly, EHR-systems, as (broadly) defined under the EHDS, are required to also comply with the proposed Cyber Resilience Act ("CRA"), with further requirements for security.

Thirdly, medical devices that are also (or claim interoperability with) EHR systems must simultaneously comply with further requirements, including safety and security, under the Medical Devices Regulation ("MDR")[8]; and similarly, 'high-risk AI' must also comply with further requirements, including safety and security, under the proposed AI Regulation ("AIA").[9] The MDR and AIA require third party conformity assessment and the CRA requires conformity assessment according to EHDS Chapter III.[10]

Fourthly, such an overreaching definition without clear limiting characteristics is bound to lead to the inclusion of many more products and services when Member States have implemented the EHDS imposing *de facto* requirements (cf. Art 14.5).

Finally, while "general software used in a healthcare environment" is excluded, the EHDS neither defines this nor includes any relevant recital to guide the interpretation and thereby understating what may be implied. The result may be fragmentation of its interpretation and aggravation of the overlaps and compliance burdens for innovative digital technologies in health.

DIGITALEUROPE recommends:

- Particularly for EHR systems (Art 2(2)(n)), a definition that focuses on systems primarily intended by the manufacturer to store, view and share patient-related information with patients, authorised providers and healthcare professionals, and to enable data flow between healthcare providers, as well as EU Member States, which would be in line with the intended purpose of the EHDS. For this reason, EHR systems should be able to consolidate and retain health-related data in electronic form.
- Introducing a better description of what "intended purpose" would constitute an EHR system, reflecting the notion of systems intended to store and share patient-related information with authorised providers and healthcare professionals and to enable data flow between healthcare providers, as well as EU Member States.
- The definition of an 'EHR' itself (Art (2)(m)) would benefit from further clarification, by focusing on some of the main features of EHRs, namely

[8] The CRA is intended to exclude MDR (Regulation (EU) 2017/745) and In *Vitro* Diagnostic Devices Regulation (IVDR) regulated products and services from its scope (cf. CRA Recital 12).

[9] AI Act (COM/2021/206 final)

[10] Article 24(4) of the CRA states that "Manufacturers of products with digital elements that are classified as EHR systems under the scope of [the EHDS] shall demonstrate conformity with the essential requirements laid down in Annex I of this Regulation using the relevant conformity assessment procedure as required by [Chapter III of the EHDS]".

its centralising nature of data being collected from different sources, as well as it being retained by or on behalf of the health system. In particular, it should be made clear that not all locations where health information is generated or resides is part of the EHR of a natural person.

- The EHDS should either define “general software used in a healthcare environment” (Art 14(2)) and/or further specify how “use in a healthcare environment” should be interpreted in practice.

Clarify delineation, simplify interplay and compliance

Manufacturers of medical devices and providers of high-risk AI systems (as defined in the proposed AI Act) ‘claiming interoperability with the EHR systems’ – as delineated by the current text but to be further clarified if the intent would be for all devices that meet these definitions – will have to prove compliance with the essential requirements on interoperability set out in the EHDS proposal and the common conformity specifications to be adopted by the European Commission in an implementing act. This requirement needs clarification as to whether the EHDS proposed (technical) essential requirements for EHR systems and such medical devices/high-risk AI systems complement or diverge from the requirements under the MDR/IVDR, as well as the impact these requirements may have on compliance with those under the MDR/IVDR.

The proposed Article 14, which intends to clarify the interplay with medical devices under the MDR and high-risk AI systems proposed in the AI Act, is not clear. It needs to be clarified to prevent requiring the manufacturer to conduct conformity assessments under all three regulations (MDR, AI Act and EHDS). If nonetheless the product falls under several regulated categories, it is key to clarify which rules apply to ensure a harmonised application of the regulations and to avoid adding uncertainty.

Upon implementation, there is a risk that the EHDS may become a much more burdensome additional layer of product requirements for manufacturers of medical devices providing data for EHR systems[11]. This is particularly relevant to the medical devices sector that faces compliance obligations with an ever-growing set of regulations, such as the MDR and proposed AIA, which also require third-party conformity assessment.

Healthcare systems will expect interoperable medical devices that can be reflected in procurement and reimbursement policies linked to conformity requirements with the EHDS. In addition, manufacturers of medical devices will have to consider all the fundamental product regulations. This includes the

[11] For instance, the EHDS does not clarify the registration obligations for products under multiple product legislations (e.g. a medical device, which is also a high-risk AI system with an EHR component, would be subject to multiple similar registration obligations in potentially different databases).

MDR, the proposed AIA, and the proposed EHDS, in addition to the proposed Data Act,[12]the CRA, and many others.

There is a risk that these developments may lead not only to legal uncertainty and inconsistencies, but also to a counterproductive (potentially conflicting) over-regulation of these products.

DIGITALEUROPE recommends:

- Where a product is covered by both the specifications under Chapter III and the MDR and/or the proposed AI Act, prior coordination between concerned boards[13] should be *mandatory* to ensure consistency and appropriate derogations, including through dedicated guidance documents (Art 23(5); 23(6)).
- In support of Article 14 and to ensure legal clarity and certainty, Recital 29 should better explain that a product (hardware or software), which is an EHR system under EHDS Regulation and also falls within the definition of a medical device and/or high-risk AI under their respective regulations, should only be subject to the essential requirements on interoperability under the EHDS Regulation when the manufacturer claims interoperability with an EHR system within the meaning of the EHDS Regulation.

Globally-aligned standardisation

In relation to standardisation, common quality standards, formats, and content requirements will be essential for interoperability and to enable linking of EHR systems and other sources of health data. Adding EU specifications where international consensus standards already exist would create technical burdens on manufacturers catering to both European and other markets. Beyond alignment, the operationalisation of essential requirements and development of standards should include the relevant stakeholders to ensure the development and uptake of digital health applications supporting the EHDS.

DIGITALEUROPE recommends:

- Specifications should be commonly agreed and aligned with activities for furthering the maturity of global standardisation and harmonisation and existing standards that address different data domains (cf. Rec 17; Art 23(b); Annex II).

[12] The proposed Data Act introduces the so called “accessibility of data by design” requirement (cf. Article 3(1)), which *inter alia* should foster the sharing of data for the purposes of the EHDS.

[13] Medical Devices Coordination Group, European Artificial Intelligence Board, EHDS Board.

Wellbeing apps (Art. 31)

Wellbeing apps are part of a rapidly growing market of digitally supported therapies, trials, remote care, disease prevention and health management etc. The proposed voluntary labelling scheme would allow this burgeoning sector to further develop. The inclusion of this data in both the primary and the secondary use parts of the proposal is welcomed. However, further clarification and improvement to Article 31 on voluntary labelling of wellness applications would unlock much untapped potential.

DIGITALEUROPE recommends:

- For Article 2(2) point (o) to read: "'wellness application' means any appliance or software intended by the manufacturer to be used by a natural person for processing electronic health data for other purposes than, *but related to* healthcare, such as well-being and pursuing healthy life-styles;" This amendment would improve the necessary outer confines.
- On data generated by wellbeing apps, to provide clarifications. Firstly, it is not clear whether data generated by wellbeing apps can be fed into an EHR system (Annex II, 2.3). Secondly, data quality requirements should reflect different source, purpose and usage of data. For instance, a wellbeing app is not always a medical device, and data from wellbeing apps is generally not directly used for diagnostics or treatment. Data quality requirements may be different from those under the MDR.
- Requiring the voluntary label to be "placed on the device" does not bring specific practical, economic or environmental benefits, because the applications are often developed by third parties and can be downloaded on the device after an end user purchases the device. Therefore, there should be no requirement for the label to be placed on the device, but it should instead be allowed for the label to be shown in the application itself or included in companion documents (cf. Art 31(6)). Moreover, there is no obvious need for a physical form of the label to be provided by the distributor, considering that the application can be distributed via a virtual store.

Secondary use of electronic health data

DIGITALEUROPE, together with a group of 35 stakeholders, including medical professional and research organisations, patient representatives, industry associations and existing data collaborations, emphasised that the EHDS is key to rapidly scale up well-governed access to health data for the delivery of healthcare services, but also for a wide range of secondary use purposes for better health outcomes. This would increase Europe's capability and global

competitiveness for research and innovation, as well as strengthen its health systems and public health resilience.

Chapter IV of the EHDS has the right ingredients to be that game-changer: to securely unlock the potential of health data, promote the health data economy, and ensure data quality and trust. In this chapter, we highlight several areas that will require finetuning in the proposal to enable realise the objectives in a harmonised way.

General conditions

Data types (Art. 33)

DIGITALEUROPE welcomes the broad scope of data types included in the minimum categories of electronic data for secondary use, because this would allow maximising health-related insights through the combination of currently siloed data sets. However, we see the need for some critical clarifications.

It should be noted that for some of these data categories, legislation already exists (notably the Clinical Trials Regulation (CTR)). Furthermore, the inclusion of device- or person-generated electronic health data would mean that huge (often low-quality) data sets would become available for secondary use, which would make deriving insights from them difficult for all EHDS participants.

On a general note, before permits are issued and large data sets *must* be transmitted, incurring costs and potential risks, the entity that generated the data, considered either the ‘data holder’ or ‘data user’, should be involved. This entity will have key insight into the utility of the data in question, considering quality, integrity and efficiency, which can have different implications per category and re-use purposes. Other entities, such as processors, should be informed if the data contains their IP or trade secrets.

At the same time, this should not place a disproportionate burden on the data holder or data user. The data that can be shared should strike the right balance between its utility and the resources required to achieve the intended purpose of the processing, while respecting IP and trade secrets, to ensure Europe remains competitive for investment and research.

Some data sets are more shareable than others. For instance, there is a significant difference between sharable raw data, which refers to clinical measurements/values common to all manufacturers, and proprietary raw data, corresponding to specific, machine-readable measurements, which have been gathered using specific IP and add a value to the manufacturer’s specific device.

DIGITALEUROPE recommends:

- Clarify in a recital whether the following data types are included: patient-reported outcomes measures (PROMs), patient-reported experience measures (PREMs), surgical audios/videos, and real world data (RWD).
- If Article (33)(1)(j) on clinical trials data is maintained in the list of the data categories, trial sponsors should act as the data holder.[14] Disclosure requirements for trial data should align to existing EU policies,[15] and not duplicate existing practices, which balance making data available with the need to protect the validity of trials and respect IP rights (as set out in the section below).
- Article (33)(1)(k) to specify that this only concerns "medicine and medical device registries", meaning, for instance, that it does not cover data originating directly from devices.
- Avoid overflowing the EHDS with too large, incomprehensible and granular proprietary raw data sets, allowing companies to, where possible, provide an alternative to proprietary raw data sets and instead contribute actionable data – data summarised and/or interpreted to be easily read and understood and processed by the user.
- Any future changes to the list of data types (currently allowed via delegated act) would benefit from public scrutiny and consultation with all stakeholders, including industry.

Purposes (Art. 34)

DIGITALEUROPE welcomes the inclusion of both the public and the private sector in the valid purposes of access (Art. 34 (a)-(h)) in recognition of the critical role small and large companies play in improving healthcare delivery for patients and their families.

At the same time, we note that there is a significant potential for deployment of data for purposes other than research and development of new technologies. Health economic and outcomes research studies serve to inform reimbursement processes, using RWD for better understanding and a more complete picture of patients' health journeys and the effectiveness of health interventions outside of the tightly-controlled settings of clinical trials.

DIGITALEUROPE recommends:

- Including in Article 34(1)(f) development and innovation activities for products or services contributing to public health, care or well-being or

[14] Or if it is not based in the EU, the EU legal representative.

[15] The GDPR, EU Clinical Trials Regulation EU No. 536/2014 and European Medicines Agency (EMA) Policies 0070 and EFPIA principles for sharing of clinical trial information.

social security, or ensuring high levels of quality and safety of health care, of medicinal products or medical devices;

- Clarifying in a recital whether the following purposes are included: supporting operational efficiency (i.e., improving delivery of care and reliability of product flow, including across borders); improving the patient pathway; post-market monitoring to identify side effects and adverse events.
- Explicitly including health economics and outcomes research in the list of valid purposes of access.

For the valid purposes for access by public bodies (Art 34(1)(a) to (c)):

- The notion of "public interest" is undefined and would benefit from specifying cases of serious public health threats to provide more legal clarity.
- The proposal should also avoid creating situations where industry takes on duties that are part of public authorities' mandates.

Prohibited uses (Art. 35)

DIGITALEUROPE recommends:

- Further clarification of the prohibited secondary uses of electronic health data under the permitting system, as the current list is too broad and could have unintended consequences (e.g. affect the testing of AI models in the context of R&D activities, prevent profiling aimed at improving patient health, or hamper market research).
- Including a prohibition on the use of shared data (or the results or output of the use of the shared data) for "unfair commercial and/or unfair competitive use" as set out in Article 39 of TRIPS (on the protection of undisclosed information), which links also to Article 10bis of the Paris Convention (on unfair competition). An additional prohibited use should also be added forbidding data users from using data obtained on the basis of a data permit or data request to reverse engineer a product/service that competes with the product of a data holder from which the data originates, in line with the Data Act.

Limits to the scope of the permitting system

On a more general note, the EHDS should allow the continuation of bilateral and multilateral, voluntary contractual relationships outside the EHDS framework, rather than making data sharing exclusively possible by way of obtaining a permit the data holder or the health data access bodies (HDABs), which risks causing bottlenecks. Existing agreements and partnerships should also continue, based on the existing legal, contractual and/or voluntary frameworks.

In the above-mentioned consensus statement, we argue that existing health data infrastructures must be leveraged to allow continuity and build on existing expertise. The European Commission, Member States and other stakeholders have in recent years invested considerable finance and resources in many health and research data infrastructures and registries that have established data flows, technical architectures, governance models and data access.

To avoid unnecessary bottlenecks, we strongly recommend that a level of continuity be maintained with initiatives where data collaboration is working today. This will allow for communities of practice that already have this relevant expertise and experience, and the methodologies that have already been proven to be utilised when implementing the EHDS.

The text, as it stands, does not make this sufficiently clear and is at times ambiguous on this point. In particular under Article 49(1), the phrase “by way of derogation from Article 45(1)” could be read to imply that making an application under Article 45 (covering data access applications to the HDAB) or under Article 49 (access to electronic health data from a single data holder) are the only ways for a data user to access electronic health data for re-use. This notion is further reinforced by the subsequent sentence stating that “multi-country requests and requests requiring a combination of datasets from several data holders shall be addressed to HDABs”.

DIGITALEUROPE recommends:

- Including a clarification that the data permit system provides for a complementary path to increased data sharing.

Intellectual property and trade secrets

As it stands, the proposal requires private enterprises to provide access to their data even if it is protected by intellectual property rights or trade secrets. Whilst the proposal states measures will be taken to protect these rights, it is unclear what these would be and whether they would be sufficient or enforceable.

Otherwise, this appears to undermine the rights of IP owners and trade secret holders who have gathered data through their own efforts, creativity and with substantial investments, and weakens the ability of private enterprises to take risks and invest in the very type of innovation the EHDS aims to stimulate.

Proper limits to data availability must be incorporated to avert incentives for data misuse and anticompetitive behaviour.

DIGITALEUROPE recommends:

- Amending the proposal so it neither seeks to create exceptions to, nor rewrite, IP and trade secret laws (including the right of a party to retain and protect information as confidential), and rather respects the role and prevalence of those laws and rights over the proposed Regulation.

- Preserving and respecting 1) the ability of private enterprises to protect IP and trade secrets (including confidentiality rights) in data sets that are in the scope of the EHDS and 2) private enterprises' right of self-determination in making data available under the proposed Regulation. Avoiding obligations for disclosure by private enterprises of data protected by IP and trade secret confidentiality empowers private enterprises to choose voluntarily and contractually make their IP and trade secret protected data available on fair and reasonable terms based on the negotiations between data holders and data users.
- Give data holders the right to include in data permits (1) fair and reasonable terms concerning use by data users of the shared data and any results and output created by the data user, for instance, to protect the IP, trade secrets and confidential information of the data holder (e.g. against disclosure, reverse engineering or any activity resulting in any diminution of those rights), and (2) a prohibition on use by the data user of the shared data or the results or output for unfair competition/unfair commercial use, and (3) not share data with anyone who will not agree to (or breaches) these data permit terms.
- We call for a new provision setting out the duties for data users, akin to the duties for data holders under Article 41, which includes respecting IP and trade secrets, and setting appropriate penalties against misuse of data.

Publicising research

The HDABs shall make public all data permit requests within 30 days (Art 37(1)(q)(ii)), and data users shall make public the results or output of the secondary use of electronic health data (Art 46(11)). These provisions do not sufficiently address confidentiality needed to avoid unintended consequences due to competitive analysis and privacy breach in conducting research.

In addition, HDABs are only obliged to inform the data holder about the use and enrichment of the data sets they originally put into EHDS. Given the current definition of the data holder, the processor will consequently remain out of the information sharing loop. A processor could be, for instance, the manufacturer of the device that originally recorded the data.

DIGITALEUROPE recommends:

- Solely having the high-level HDAB activity annual report would be a better alternative that would provide transparency of activities whilst still protecting commercial incentives, also resulting in reduced burden on HDABs (Cf. Rec 44; Art 39).
- Similarly, the obligation for data users to make public the results of any research using EHDS data 18 months after its provision should clarify how the data user can protect their, and the original data holder's IP

and competitive intelligence. This is especially relevant in a scenario where such disclosure would also entail the input data from the data holder. One way of solving this issue would be to distinguish scientific research by public bodies from R&D performed by private enterprises.

- Data processors should have the same rights as data holders, in being informed about enrichment of their data sets as set out in Article 37(1)(p).

Dispute mechanism

The proposal is lacking a process for data holders to fairly contest requests, for instance, if they believe it represents confidential information and/or a trade secret, considering European and Member State laws and protecting due process rights.

DIGITALEUROPE recommends:

- Including in a provision among the rights for data holders to refuse access if they provide justification (Art 41), deemed as sufficient by the relevant HDAB.
- Including a clause stipulating that in business-to-government context, the data applicant must provide sufficient evidence that it could not obtain the data by other means (cf. Article 15(1)(c) of the proposed Data Act where such a requirement is included for exceptional needs by public bodies).
- Introducing a more general dispute resolution mechanism in the proposal for data holders, requesters, users, and other involved actors, since judicial remedies can take time and thus hinder innovation. This could be used, amongst other purposes, to dispute the requirement to disclose IP right- and trade secret-protected data or help resolve issues between single data holders and data users, and build on the proposed mechanism under Article 42(4), which currently focuses solely on disputes concerning fees (and which itself is based on the Data Act proposal's mechanism in Article 10).

Governance and process

Timeframes and default decisions

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. Additionally, the current default option to grant the permit is clearly a less appropriate option to incentivise 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.

DIGITALEUROPE recommends:

- Exploring ways to improve compliance and operationalisation to allow data holders to have sufficient time to review any comments received by the HDAB.
- In alignment with existing legislation on clinical trial data, for that category (Article 33(1)(j)), the duration of data permit should be 18 months (standard industry practice).
- The default position in these cases should be that the permit is not granted to avoid data being shared without sufficient review of the request (cf. Art 46(3)).
- By the same token, whereas it is stipulated in Article 48 that public bodies shall not require a permit for purposes listed in Articles 37(1)(a) and 37(1)(c), we strongly recommend that they should not be able to access privately held data without a permit (as supported by the EDPB/EDPS Joint Opinion in paragraph 99). In case of emergencies, these should be further clarified (see above) and aligned with the Data Act.

Fees and penalties

Provisions on fees and compensation are still unclear, and this would require further study of the economic sustainability of the EHDS.

DIGITALEUROPE recommends:

- For the fee structure to be harmonised and proportionate to the data type, quality, size of the dataset and its intended use, rather than the size of the organisation (cf. Article 42). Fees should not just be “transparent and proportionate”, but rather based on fair market value remuneration for data collection costs by data holders and data recipients agreeing suitable contractual and compensation terms. Fees for anonymisation and pseudonymisation, where needed, should not be borne by the data holder providing the data.
- Provide more clarity on what authority will be in charge to evaluate and decide whether an obstruction is intentional or not, and what remedies is provided for data holders to challenge a decision (cf. Art 43).
- Clarification is needed on the structure of the fines, and on whether preventing participation in the EHDS would also prevent access to data from single data holders, and from having to make data available via a direct request.

Health data access bodies

The EHDS’s success is dependent on providing European alignment on health data access and governance, and for this reason national health data access

bodies (HDABs) will be an important element which can help the system be more agile, responsive, and efficient. From the data holders' and data users' side, the clearer the process is in the legal text, the more predictable and acceptable the EHDS will be, if the conditions are non-discriminatory, fair, transparent and proportionate.

Moreover, the HDABs will perform certain tasks intended to improve "the original database" (Recital 39) by sending "to the data holder free of charge, by the expiry of the data permit, a copy of the corrected, annotated or enriched dataset, as applicable, and a description of the operations performed on the original dataset" (Article 37(1)(p)).

The operational part of the proposal remains too ambiguous as to what the mechanism would look like. Note that in Recital 39 it is stated that the data holder should "make available" the data, while Article 37 requires "sending" the data. Finally, it is prescribed that the original data holder may notify the HDAB that it does not wish to make available the enriched dataset, for instance due to low quality. This is neither the most efficient nor the safest mechanism, because the data users and the HDAB have much better insight into the processing that took place.

DIGITALEUROPE recommends:

- Sufficient funding must be committed to establishing HDABs in all Member States. This must be required in the legal text.
- Competencies should be further defined in relation to those of data protection authorities to avoid duplication and confusion.
- The HDABs' role should also include providing a certain level of technical traceability between the used datasets and the source data (in full respect of privacy), where this is a requirement for regulatory or HTA submissions.
- 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 harmonised 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.
- The Commission's template for joint controllers' arrangement (cf. Articles 49 and 51) between HDABs and data users should clarify the limits of liability over the lawfulness of personal data that the data user

will be compelled to assume and should clarify the obligations of the controller vis-à-vis the data holder. This template should also be extended to cases where data users are joint controllers with single data holders to provide legal certainty.

- Including a mechanism for the HDAB to first report what would be beneficial systemically to the original data holder (e.g. in managing and improving EHR completion) instead of simply sending (all) the data back.[16] This would also remove an unnecessary burden from data users. If the aim of this mechanism is to support scientific activity (cf. Recital 39), this should be reflected in the operational part.[17] If the intended purpose is not taken into account, this could lead to serious issues downstream. "Data wrangling" may be necessary to produce valid datasets for machine learning, which are not suited for clinical use and much more complex than error correction of EHR data.

Single data holders (Art. 49)

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.

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.

DIGITALEUROPE recommends:

- 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.
- Clarifying 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.

[16] Reporting is essential for instance to distinguish between data quality (a focus on populations, acknowledging error in individual data points) and data integrity (focus on individual data points – in this case of EHR data).

[17] Such a mechanism may draw inspiration from those offered by DARWIN EU and specifically the EHDEN project such as the Data Quality Dashboard_ODHSI-EHDEN.

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.

In the consensus statement mentioned in the introduction, 35 stakeholders strongly underline the need for approvals for secondary use of health data to be consistent and harmonised across Europe. Together, we recommend that, generally, legal and ethical criteria for approving pseudonymised data use and data linkage 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 full 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.[18]

DIGITALEUROPE recommends:

- 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 ‘sufficient anonymisation’. We therefore advocate for the recognition of risk-based 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.[19]

[18] Digital Public Health (2022) Selecting Privacy-Enhancing Technologies for Managing Health Data Use

[19] https://www.appliedclinicaltrialsonline.com/view/sharing-anonymized-and-functionally-effective-safe-data-standard-for-safely-sharing-rich-clinical-trial-data

- Similarly, 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 and without re-identifying the individual, 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.
- The key to reversing pseudonymisation should be held not by the HDABs, but by data holders for maximum data protection (cf. Recital 49).

Additional requirements for data holders and data users

Data holders (Art. 41)

DIGITALEUROPE recommends:

- Defining in Art 41(2) more clearly that the “data holder shall communicate to the health data access body a general description of the dataset it holds in accordance with Article 55” should be required at a level of generalisation that is proportionate so as to not overburden data holders nor the HDABs. It will be particularly challenging for large organisations and access nodes to identify and access all the data they hold or is held in their jurisdiction.
- The request for data holders to make non-personal electronic health data available in “trusted open databases for unrestricted access” (cf. Article 41(6)) needs clarification on which parties are in scope, reassurance that there is no requirement for data holders to invest in developing such databases, and confirmation that data does not need to be translated to all languages for accessibility. One solution would be to state that data held by private companies would not be in scope of this obligation.
- In Article 46 on data permits, it must be clarified to what extent data holders are involved in the decision to grant a permit, and more generally it is not clear which principles will be used by the HDAB to grant a permit or not.

Data users

DIGITALEUROPE recommends:

- Adding more detail on the requirements for sending back enriched data (Article 37(1)(p)). For instance, what if the data request has used data from different sources? There should be clear criteria of what constitutes an “improvement” that must be returned to the data holder and the processor where relevant, when this must be returned, and any obligations of the data holder related to the enriched data. See also the section on health data access bodies.
- A new provision setting out the duties for data users, akin to the duties for data holders in Article 41, as mentioned in the segment on IP and trade secrets.

Implementation

Implementing acts

Implementing acts are omnipresent in the proposal, especially regarding the technical specifications for some of the most important obligations, such as the rights of natural persons in relation to the primary use of their health data (Article 3(12)), European electronic health record exchange format (Article 6), registration of personal electronic health data (Article 7(3)), identification management (Article 9(2)), common specifications (Article 23(1)), label of wellness apps (Article 31(3)), etc.

Without knowing the technical details of the rights and obligations of individuals or the industry, it will be very difficult to provide feedback as to the feasibility of the obligations. Particularly, the data holders should provide certain information for the dataset catalogue, but due to hardly any information provided in the proposed legislation, it is difficult to comment the administrative burden for the industry.

DIGITALEUROPE recommends:

- As much as possible information should be provided about the technical specifications at this point of time and only foresee a right to update these obligations in order to avoid further fragmentation.

Allocation of tasks between relevant bodies

The proposals’ operational blueprint should avoid further complicating the landscape for governance and enforcement, including surveillance, compliance, permitting and dispute settlement. Given the developing data

legislation landscape, there is a growing concern regarding consistency.[20] Strictly looking at the data legislation, there are supervisory authorities under the GDPR, competent authorities under the Data Act, and digital health authorities and HDABs under the EHDS.

Moreover, looking at the operational framework for the product legislation under Chapter III, the notion of multiple competent authorities, considering their establishment and operationalisation (not to mention potentially divergent approaches and agendas), may give rise to serious compliance challenges for companies, but also represent unnecessarily high and duplicated cost to society and taxpayers.

DIGITALEUROPE recommends:

- An approach that combines the digital health authorities, or at least their tasks, under Chapter III, with the existing ones to avoid unnecessary and costly proliferation of additional entities (cf. Article 10).

Market-driven standardisation

The proposal contains a raft of standards and common specification to be developed.[21] Harmonised standards have not been sufficiently considered. Open, voluntary, market-driven consensus-based standards are the best way to facilitate innovation that is at least on-par with international developments and is ready to be exported outside of Europe.[22]

DIGITALEUROPE recommends:

- The standardisation framework should be a natural extension of existing structures, such as the eHealth Network and the Multi-Stakeholder Platform (MSP) for ICT standardisation, taking into account the reality of the existing global standardisation arena. In particular, harmonised standards should be prioritised and there should be a link to all relevant European and international standards development organisations (SDOs) of all sorts, including industry consortia, and not only to the legally recognised European Standardisation Organisations (CEN, CENELEC, ETSI) or their global equivalents (ISO, IEC, ITU).
- There should be, where appropriate with national arrangements, regional involvement when agreeing on standards, while maintaining coordination at the national level to avoid further complications.

[20] As was also noted in the EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act).

[21] We identified those in the form of Implementing Acts in Articles: 3(12); 6(1); 7(3); 9(2): 12(4;8); 13(1;2;3); 23(1); and 31(3).

[22] DIGITALEUROPE (2022) DIGITALEUROPE's response to the Standardisation Strategy.

Governance of the EHDS

DIGITALEUROPE welcomes the proposal to create the European Health Data Space Board that will facilitate the cooperation between digital health authorities and HDABs, and contribute to the consistent application of the EHDS regulation throughout the EU. When setting up bodies tasked with implementing the EHDS, it will be vital that all stakeholders take part in its governance, from patient associations (as improving patient wellbeing is the main goal) to research and industry (which will be the ones re-using health data for innovation).

DIGITALEUROPE recommends:

- 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.
- For health data access bodies to also cooperate with data holders in addition to stakeholders, including patient organisations, representatives from natural persons, health professionals, researchers, and ethical committees in the exercise of their tasks to ensure equal and equitable representation by all stakeholders (cf. Art 37(2)).
- In terms of review, we suggest covering all aspects of the regulation after two years – not seven – with the aim of identifying, prioritising, anticipating and solving any hurdles for implementation very early in the implementation process, and avoid unfortunate delays in the implementation, as recently experienced with the implementation of EU MDR and IVDR.[23]

[23] Regulation 2017/746 on in vitro diagnostic medical devices.

FOR MORE INFORMATION, PLEASE CONTACT:

Richard Rak

Digital Health Policy Officer

richard.rak@digitaleurope.org / +32 492 467817

Michael Strübin

Senior Advisor Digital Health

michael.strubin@digitaleurope.org / +32 491 56 94 78

Ray Pinto

Director for Digital Transformation Policy

ray.pinto@digitaleurope.org / +32 472 55 84 02

About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory environment that enables European businesses and citizens to prosper from digital technologies. We wish Europe to grow, attract, and sustain the world's best digital talents and technology companies. Together with our members, we shape the industry policy positions on all relevant legislative matters and contribute to the development and implementation of relevant EU policies, as well as international policies that have an impact on Europe's digital economy. Our membership represents over 45,000 businesses who operate and invest in Europe. It includes 96 corporations which are global leaders in their field of activity, as well as 41 national trade associations from across Europe.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Assent, Autodesk, Banco Santander, Bayer, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, CyberArk, Danfoss, Dassault Systèmes, DATEV, Dell, Eaton, Epson, Ericsson, ESET, EY, Fujitsu, GlaxoSmithKline, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, Intel, Johnson & Johnson, Johnson Controls International, Konica Minolta, Kry, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Meta, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nemetschek, NetApp, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Red Hat, RELX, ResMed, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Skillsoft, Sky CP, Sony, Sopra Steria, Swatch Group, Technicolor, Texas Instruments, TikTok, Toshiba, TP Vision, UnitedHealth Group, Visa, Vivo, VMware, Waymo, Workday, Xerox, Xiaomi, Zoom.

National Trade Associations

Austria: IOÖ
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Czech Republic: AAVIT
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, SECIMAVI, numeum
Germany: bitkom, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: Infobalt
Luxembourg: APSI
Moldova: ATIC
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS
Slovakia: ITAS
Slovenia: ICT Association of Slovenia at CCIS
Spain: Adigital, AMETIC
Sweden: TechSverige, Teknikföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT Ukraine
United Kingdom: techUK