DIGITALEUROPE

DIGITALEUROPE's response to the public consultation on the European Health Data Space

71% of survey respondents reported to the European Commission that in gaining access to data for research, they experienced "high time and interaction costs", losing valuable resources.[1]

Executive summary

DIGITALEUROPE submitted its response to the public consultation for the development of the EHDS. Its key points are:

▶▶ The EHDS should be a **constantly updated and extended health data resource**. This requires a **coordinating EU-level health data entity** and **national-level entities**, adhering to the same set of rules.

▶▶ **Clear and practical guidance on GDPR** provisions is a must.

▶▶ **Member States should cooperate** more in **using interoperable standards and eID**, delivering faster on initiatives.[2]

▶▶ **The EHDS framework should include mechanisms for industry participation and data use,** critical for medical innovation.

▶▶ **Enable artificial Intelligence** while minimising additional regulatory burden.[3]

Extended resources on this topic can be found at [Digital for Health](#)

---

[1] See the European Commission's [Assessment of the EU Member States' rules on health data in the light of GDPR](#) for an overview of the myriad of divergent health data policies in the EU, concerning GDPR implementation, but including also different requirements for data quality, security, pharmacovigilance and medical device safety (reported on page 79)

[2] DIGITALEUROPE's Executive Council for Health warns [more urgency is needed for EU health data sharing](#)

[3] Read also [DIGITALEUROPE's initial findings on the proposed AI Act.](#)

Table of contents

A well-defined infrastructure for health data processing

The EHDS proposal should **establish the legal foundation of both the EU-level health data entity** as well as **common rules for national health data entities**.[4] It should promote internationally developed standards and interoperability among, often dispersed, databases and systems, in line with FAIR (Findable, Accessible, Interoperable and Reusable) principles in data sharing and access.[5] We support a set up composed of:

▶▶ **An EU-level entity for secondary use of health data:** As a core tenet, the EU-level health data entity should promote the frictionless sharing of health data across Europe in a safe, controlled and privacy-preserving environment.

▶▶ **National health data entities:** The role of the national entities[6] should be to provide controlled data services, like healthcare information sharing and analyses.

Both EU and national entities should be able to **process multi-country requests**. The EHDS governance **framework should be clear to avoid fragmentation** among national and regional bodies.[7] However, we urge caution with new rules for (health) data processing. Instead, clear guidance is needed given that access to, and exchange of, health data – despite existing rules – remains very limited in the EU due to various applications of the General Data Protection Regulation (GDPR)[8] and health data processing rules in Member States. DIGITALEUROPE has produced detailed recommendations for making the most of the GDPR to advance health research.[9]

---

[4] Read here our February 2021 response to the EHDS Roadmap Inception Impact Assessment.

[5] It should be coherent with other legislation, in particular on data protection and the future Data Governance Act, Data Act and the governance framework of initiatives such as Gaia-X.

[6] Such as FinData and the French Health data Hub.

[7] See also the TEHDAS paper on the barriers to health data sharing and a discussion on possible governance mechanisms.

[8] Regulation (EU) 2016/679.

[9] Read for more information DIGITALEUROPE's June 2021 paper: Making the most of the GDPR to advance health research.

Promoting Interoperability

Although multiple initiatives for interoperability exist across Europe, we observe a lack of coordination and scale, as well as a fragmentation of resources and funding and an abundance of legal and privacy-related boundaries. Serving as useful examples, **current initiatives – even combined – lack the necessary scale** and further action in this direction is crucial. COVID-19 and other public health priorities have now provided examples where Member States and authorities using eID and agreeing on interoperability were able to share data in compliance with the GDPR and overcome obstacles. For example, track and tracing apps, eHDSI[10], reinforcing the ECDC mandate[11], cross-border heath threats[12], Europe's Beating Cancer Plan[13], and the Digital COVID-19 Certificate.[14]

The EHDS instrument should **ensure that Member States coordinate** the selection and endorsement of existing international standards and profiles. This must all be organised in particular with industry engagement, throughout the process. One should also consider, where appropriate with national arrangements, regional involvement in agreeing on standards, while maintaining coordination at the national level to avoid further complications.

By ensuring greater commitment to standardisation objectives, the EHDS would boost the exchange of cross-border health data across the EU and promote health data systems interoperability, while optimising scale advantages in global supply markets for healthcare IT and medical devices.

A natural extension of the standardisation framework

The standardisation framework should be a natural extension of existing structures, such as the E-health Network[15] and the Multi-Stakeholder Platform (MSP) for ICT standardisation[16], taking into account the reality of the existing global standardisation arena. In particular, there should be a link to all relevant

---

[10] More information on the eHealth Digital Service Infrastructure.

[11] The European Commission proposal to reinforce the mandate of the European Centre for Disease Prevention and Control.

[12] The European Commission proposal for stronger, more comprehensive rules on serious cross-border health threats.

[13] More information on Europe's Beating Cancer Plan.

[14] More information on the EU Digital COVID Certificate.

[15] More information on the eHealth Network, composed of members coming from all EU Member States and Norway (observer).

[16] More information on the European Multi-Stakeholder Platform for ICT standardisation.

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).

Driving growth for European SMEs

DIGITALEUROPE's membership of 35.000 businesses, both large and small, identified that there is need for interoperable standards and increased health data access for innovation. At the same time, any approach to standardisation should ensure compliance is compatible with the business case for data sharing, especially for smaller businesses.

Avoid unnecessary burdens for compliance

Demonstrating and expressing compliance to standards is multi-faceted and technically complex**. DIGITALEUROPE recommends:**

- **More urgency is needed to implement a simple consent form for ID management** for patients throughout Europe to gain access to state-of-the-art healthcare. For example, eID if rolled out and implemented harmoniously by all Member States, will empower citizens to have an increased control over their health data and Electronic Health Records and facilitate important future initiatives.[17] Such infrastructure could have enabled faster action on the Digital COVID-19 Certificates.

- **Any EU-labelling scheme for common standards and technical requirements should build on the work of the SDOs** by recommending to underpin the application of the label with evidence, provided to optimise the implementation of these approaches.

- **A certification scheme could easily become a disproportionate burden in cost and time** and could thus slow down innovation and divert resources to procedural activities with insufficient added value. Many SDOs have developed or are developing practical approaches to tackle the issue, such as hackathons, 'connectathons', providing test tools and methods. They offer test and certification schemes, including the option for vendors to perform testing in-house through a sufficiently independent organisational set-up, and where needed subjected to external audits.

---

[17] There is an opportunity to progress in this aspect through the revision of the eIDAS regulation (910/2014)

Appropriate conditions for access to data

The EHDS framework should include mechanisms for industry participation and data use because this is an inherent necessity for medical innovation. The exponential proliferation of data has the potential to transform healthcare and deliver unprecedented levels of quality and efficiency of care. Access to, control, and transmission of health data can enable improved healthcare by ensuring more effective and personalised treatment, more precise diagnostics, remote patient monitoring and individual patient-centred care.

To make this a reality, **an appropriate data governance model must be established**. This should provide measures and premises for both primary and secondary use of health data. The latter includes industry, medical technology, pharmaceutical innovations, and other health solutions, which need data to develop and demonstrate efficacy and safety of products and services; for example, during market surveillance activities to ensure transparency.

The public sector already has a great amount of data, which could be used in much more efficient ways.[18] Therefore, in a first step, **Member States must ensure that they make the best use of existing data they hold**. It should be noted that data that needs considerable cleaning of invalid values and/or normalisation of multiple codes for the same concept into one code generally has a lower benefit than high quality data.

The optimal mechanisms for health data access would depend, among other things, on whether it concerns patients' health data records or data from clinical studies. **Citizens should be in control of their personal health data**.[19] Publicly held personal health data for which (re)use consent has been given (or pseudonymised/ anonymised health data), should be efficiently accessible, such as for important research in the public interest.

Enabling trustworthy AI-powered digital health

Industry access to health data is key for training testing and validating a well-functioning AI system. Now, data access is fragmented, and its utility is greatly reduced by lack of interoperability. Specific needs should be defined to support the training, testing and validation of AI, such as the management of bias. High quality, high-volume, accurate, sufficiently representative, and properly annotated data sets which meet the required standards for clinical evidence

---

[18] EMERJ (2019). Where Healthcare's Big Data Actually Comes From

[19] For citizens to be in control of their data the Commission should fulfil its ambitions for the Recommendation on a European Electronic Health Record exchange format (2019/243)

would be essential for developing robust, unbiased, and ethically sound AI-enabled medical products or services.

It must be noted that ethical issues with AI, such as biased outcomes, are not unique to healthcare. Some healthcare applications will be high risk, and some will be low risk, as with other sectors, and a proportionate approach needs to be taken; we argue for a **case-by-case approach**. Many ethical issues occurring in health applications of AI are already mitigated by the existing legislative framework. For medical devices, existing regulation already increasingly aims to address ethical concerns, such as ensuring that discrimination, bias, errors are tackled at the design stage, as well as validation and during any medical device's life cycle.

Two areas where AI applied in health can, in some cases, have specific ethical concerns can, to a large extent, be mitigated through better data access, curation and understanding of health data. This is needed to:

▶▶ **Counter discrimination:** AI systems are based on data. The lack of access to adequate representative datasets for the intended population may lead to bias. Data access and processing mechanisms should be provided to ensure that negative or undesired bias is properly managed.

▶▶ **Increase explainability:** A lack of proper understanding of what the AI system does and does not would lead to inefficient use of and mistrust the system. Healthcare professionals should have the skills to understand the outputs of the system and explain them to patients. Additionally, proportionality is key to the discussion on the explainability of AI decisions specifically with respect to the intended use of the technology, and the corresponding potential risk for the patient. The aim should be to provide meaningful insights.

Finally, **AI powered approaches may require review protocols, organisational arrangements and redefining roles**. Although it depends on the type of AI and intended purpose (not every AI will create new relationships), certain systems will imply new approaches enhancing medical practice and improving healthcare professional and patient's experience (e.g., faster and more accurate diagnosis, better vision during surgery, smarter triage of patients).

DIGITALEUROPE will continue to work on policy insights and recommendations for the realisation of an ambitious and timely EHDS, notably with its Executive Council for Health which has taken this up as a priority.

FOR MORE INFORMATION, PLEASE CONTACT:

Ray Pinto

Digital Transformation Policy Director

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

Thomas Hellebrand

Policy Officer Digital Transformation

thomas.hellebrand@digitaleurope.org / +32 492 46 78 17

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Assent, Atos, Autodesk, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Eli Lilly and Company, Epson, Ericsson, ESET, Facebook, Fujitsu, GlaxoSmithKline, Global Knowledge, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, NetApp, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Red Hat, ResMed, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sky CP, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, UnitedHealth Group, Visa, VMware, Waymo, Workday, Xerox, Xiaomi, Zoom.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
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
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE

Romania: ANIS
Slovakia: ITAS
Slovenia: ICT Association of Slovenia at CCIS
Spain: AMETIC
Sweden: Teknikföretagen, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
United Kingdom: techUK