ALERT MEMORANDUM

European Health Data Space – The Commission's Proposal on a Single Market For Digital Health Services, Products, and Data

July 19, 2022

On May 3, 2022, the European Commission (the "**Commission**") published its proposal for a regulation on the "European Health Data Space" (the "**Regulation**" and the "**EHDS**").

The EHDS is a talismanic European healthtech initiative that could revolutionize access to a deeper pool of EU-wide health data and unlock significant tech, AI and data analytics innovation. As a core part of the Commission's European Data Strategy, the EHDS seeks to tackle legacy systemic issues that have hindered lawful access to electronic health data. The Regulation strives to create a "European Health Union" by strengthening individuals' access to and portability of their electronic health data and allowing innovators and researchers to process this data through reliable and secure mechanisms. It is worth noting that the EHDS proposal does not to create (nor could it feasibly do so) a unitary central EU database of electronic health data, but seeks to facilitate multilateral exchange of such health data from decentralized databases through the EHDS's regulatory infrastructure.

The EHDS proposal builds upon other recent and contemporaneous EU data and healthcare reforms, such as Regulation (EU) 2017/745 on medical devices,[1] the proposed AI Act,[2] the Data Governance Act,[3] and the proposed Data Act[4]. It presents a welcome opportunity to resolve areas of uncertainty as to the lawful bases for health data processing under Regulation (EU) 2016/679 ("GDPR")[5] and fragmented Member State national laws that might otherwise inhibit "big data" innovation in the European healthcare sector. However, work remains to be done to reconcile areas of legislative interplay and ensure that data subjects' GDPR rights remain protected.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors

ROME
Piazza di Spagna 15
00187 Rome, Italy
T: +39 06 69 52 21

Federica Mammì Borruto
+39 06 6952 2826
fmammiborruto@cgsh.com

LONDON
2 London Wall Place
London EC2Y 5AU
T: +44 20 7614 2200

Gareth Kristensen
+44 20 7614 2381
gkristensen@cgsh.com

[1] Regulation (EU) 2017/745 of the European Parliament and of the Council of April 5, 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC [2017] OJ L 117.

[2] Proposal for a Regulation laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) COM/2021/206 final.

[3] Regulation (EU) 2022/868 of the European Parliament and of the Council of May 30, 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) [2022] OJ L 152.

[4] Proposal for a Regulation on harmonized rules on fair access and use of data (Data Act) COM/2022/068 final.

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119.

© Cleary Gottlieb Steen & Hamilton LLP, 2022. All rights reserved.
This memorandum was prepared as a service to clients and other friends of Cleary Gottlieb to report on recent developments that may be of interest to them. The information in it is therefore general, and should not be considered or relied on as legal advice. Throughout this memorandum, "Cleary Gottlieb" and the "firm" refer to Cleary Gottlieb Steen & Hamilton LLP and its affiliated entities in certain jurisdictions, and the term "offices" includes offices of those affiliated entities.

I. Overview of the EHDS

The Commission's EHDS proposal seeks to benefit citizens, healthcare professionals, researchers, industries, regulators and policy-makers by "*unleash*[ing] *the full potential of health data*"[6]. The core aims of the Regulation are to:

- strengthen individuals' control over their health data (including electronic health records, health data from apps and medical devices, and health data contained in registries) through the free flow of data and improved access in electronic format by healthcare professionals;
- foster a single market for digital health services and products, electronic health record ("**EHR**") systems,[7] and high-risk AI systems; and
- establish clear rules for a trustworthy processing of individuals' non-identifiable health data for research, innovation and regulatory purposes.

To reach these goals, the proposed Regulation sets up cross-border infrastructures that enable the primary uses (*i.e.*, the provision of healthcare services to individuals) and secondary uses (*i.e.*, research, innovation, regulatory and policymaking purposes) of electronic health data (e.g., patient summaries, electronic prescriptions or dispensations, medical images, laboratory results, and discharge reports), and introduces mandatory requirements for healthcare providers, researchers, and businesses, including when they employ artificial intelligence systems.

The Regulation will apply to: *(i)* manufacturers and suppliers of EHR systems and wellness applications within the EU and users of such products; *(ii)* controllers and processors established in the EU processing electronic health data of EU citizens and third-country nationals legally residing in Member States; *(iii)* controllers and processors established in a third country[8] that have been connected to or are interoperable with the central digital health platform called "MyHealth@EU";[9] and *(iv)* data users to whom data holders provide electronic health data in the EU.[10]

II. Primary use of electronic health data

Chapters II and III of the Regulation aim to define the rights of individuals regarding their electronic health data (to complement GDPR provisions), list the obligations of healthcare professionals, implement a self-certification scheme for EHR systems to ensure interoperability and security, and introduce voluntary labeling of wellness applications interoperable with EHR systems.

Individuals have the right to access their electronic personal health data, "*immediately, free of charge and in an easily readable, consolidated and accessible form*".[11] Moreover, the right to data portability under Article 3(2) of the Regulation applies to all electronic health data, thus extending to non-personal health data (at least to the priority categories listed in Article 5 of the Regulation). In the case of personal health data that have not been registered electronically prior to the application of the Regulation, Member States may require that this data nevertheless be provided in electronic format pursuant to Article 3 of the Regulation.

Electronic health data access services must ensure the exercise of rights at the national, regional or local level, and proxy services must allow individuals to authorize others (such as guardians or representatives) to access their electronic health data on their behalf automatically or upon request. Electronic health data access services must also allow individuals to request online rectification of data under Article 16 of the GDPR.

[6] https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en.

[7] EHR systems are defined as "*any appliance or software intended by the manufacturer to be used for storing, intermediating, importing, exporting, converting, editing or viewing electronic health records*" (see Article 2(2)(n) of the Regulation).

[8] The Regulation does not provide a definition of "third country". However, according to EU legislation, this term should identify countries outside the European Economic Area.

[9] See Article 12 of the Regulation.

[10] Article 1(3) of the Regulation.

[11] Article 3(1) of the Regulation.

Notwithstanding Article 6(1)(d) of the GDPR[12] and the rules and safeguards established by Member States, individuals can restrict healthcare professionals' access to all or part of their electronic health data. Individuals also have the right to receive information about healthcare providers or healthcare professionals who have accessed their electronic health data in the context of healthcare.

In the event of non-compliance, data protection supervisory authorities can impose administrative fines up to 20,000,000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher, pursuant to Article 83(5) of the GDPR.[13]

Healthcare professionals have the right to access electronic health data of individuals under their treatment "*irrespective of the Member State of affiliation and the Member State of treatment*"[14], unless individuals have restricted access to such data (in these situations individuals must provide prior authorization), and must ensure that this data are kept up-to-date with the health services provided. Access to restricted data is allowed only if it is necessary to protect the vital interests of the data subject or of another individual.[15] Through implementing acts, the Commission will have to identify the exchange format and the requirements for recording of electronic health data. Cross-border identification will be ensured by mechanisms in accordance with eIDAS Regulation,[16] especially in case of telemedicine services or access to personal health data.[17] However, at this stage it is not yet clear how the technical implementation of national access services will work in practice (also considering the discretion of Member States in the development of such access services), as well as how interconnection with electronic identification procedures will be ensured.

The EU's "MyHealth@EU" platform will facilitate the exchange of electronic health data between contact points for digital health across the EU (which will act as joint controllers of electronic health data communicated through the platform "MyHealth@EU", while the Commission will be qualified as a processor), and Member States will need to ensure that all healthcare providers are connected to these national contact points.[18] Following a compliance review, the Commission can adopt implementing acts certifying the compliance of a national contact point of a third country or an international system with the requirements of the "MyHealth@EU" platform to ensure its international interoperability.[19]

Chapter III contains a list of obligations for manufacturers, importers, and distributors of EHR systems, as well as the conformity criteria of EHR systems (supplemented by Annex II). Moreover, manufacturers of wellness applications that are interoperable with an EHR system (with the exception of applications that are high-risk AI systems) may use a label indicating their compliance with the Regulation, the validity of which does not exceed five years.[20] The Commission will maintain a public database with information on EHR systems that have obtained an EU declaration of conformity or wellness applications for which a label has been issued.[21]

[12] Processing is necessary in order to protect the vital interests of the data subject or of another natural person.

[13] In addition, Member States must designate a digital health authority responsible for the implementation and enforcement of the Regulation at national level (see Article 10), with which natural and legal persons have the right to lodge a complaint (see Article 11). To enhance cooperation and information exchange among Member States, a European Health Data Space Board, composed of high-level representatives of digital health authorities and health data access bodies, will also be established (see Article 64).

[14] Article 4(1) of the Regulation.

[15] Article 4(4) of the Regulation.

[16] Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L 257.

[17] Article 9 of the Regulation.

[18] Article 12 of the Regulation. Other infrastructures, including the Clinical Patient Management System, can become authorized participants in the platform "MyHealth@EU" pursuant to Article 13(2) of the Regulation.

[19] Article 13(3) of the Regulation.

[20] Article 31 of the Regulation.

[21] Article 32 of the Regulation.

Main obligations of economic operators regarding EHR systems

- Do not mislead users about the purpose, functions, interoperability, and security of EHR systems, including by omitting information about potential limitations or suggesting uses other than those stated in their technical documentation.
- Ensure and declare conformity of EHR systems with the requirements set forth in the Regulation through technical documentation or take any necessary corrective action (including recall or withdrawal of such systems), provide users with instructions for use, and affix CE marking.
- Cooperate with market surveillance authorities (*i.e.*, generally with digital health authorities under Article 10 of the Regulation).
- Do not alter the EHR system in such a way as to compromise conformity.
- Notify any serious incident involving an EHR system to the market surveillance authorities of the Member States where the incident occurred.

III. Secondary uses of electronic health data

Chapters IV and V of the Regulation are devoted to secondary uses of electronic health data for research, innovation, and policymaking purposes by data users[22], who may request access to such data from data holders.[23] The categories of electronic data that can be shared are broadly listed in Article 33 of the Regulation. However, entities that obtain access to data involving IP rights or trade secrets must ensure the confidentiality of this data.[24] Article 35 of the Regulation specifies the prohibited secondary uses of electronic health data, which must not be used to:

- make decisions (which produce legal effects or similarly significantly affect individuals) to the detriment of such individuals on the basis of their electronic health data or excluding individuals or groups of individuals from the benefit of an insurance contract or modifying their contributions and insurance premiums;
- carry out advertising or marketing activities towards healthcare professionals, healthcare organizations or individuals;
- make electronic health data available to third parties not mentioned in the data permit; or
- develop products or services that may harm individuals and society at large or goods or services that contravene public order or morality.

Member States will designate one or more health data access bodies ("**HDAB**"), which will carry out several tasks in the context of the EHDS, including granting access to electronic health data for secondary use.[25] In case of various HDABs, a coordinator should be identified.

Procedure for data permits[26]

- Any natural or legal person can submit an application for data access to an HDAB (or to a single data holder in a single Member State), containing, *inter alia*, a detailed explanation of the intended uses of electronic health data for the purposes listed in Article 34 of the Regulation, their format and source,

[22] The term "data users" includes natural or legal persons who have "*lawful access to personal or non-personal electronic health data for secondary use*" pursuing activities for reasons of public interest (see Articles 2(2)(z) and 34 of the Regulation).

[23] They mean any "*entity or a body in the health or care sector, or performing research in relation to these sectors*", as well as EU institutions, bodies, offices and agencies who has the right or obligation or the ability to make certain data available (see Article 2(2)(y) of the Regulation).

[24] Article 34(4) of the Regulation.

[25] Articles 36 and 37 of the Regulation.

[26] Articles 46-49 of the Regulation.

the safeguards envisaged, and an estimate of the processing period.

- A single application can be submitted in case electronic health data is stored in more than one Member State and the chosen HDAB must then share the request with other HDABs in the platform "HealthData@EU".
- Electronic health data is provided in an anonymized format, unless the data user provides an explanation of the reasons for seeking access to such data in a pseudonymized format. The HDAB will retain the information necessary to reverse the pseudonymization and data users will not be allowed to attempt to re-identify the data subjects.
- After evaluation by the HDAB, a data permit can be issued or refused (with a justification) within two months of receiving the data access application (this period may be extended by two additional months in the case of complex requests).
- The data permit establishes general conditions applicable to data users, including duration or technical characteristics.
- After the data permit is granted, data users can request electronic health data from data holders, which must be made available within two months of receiving the request.

HDABs and single data holders can charge fees for making electronic health data available for secondary use, based on the costs related to handling the access request process.[27]

Within eighteen months of completing the processing of electronic health data after receiving the answer to the data request under Article 47 of the Regulation, data users must publish anonymous results or output of the secondary use of data, including information relevant for the provision of healthcare.[28]

Public sector bodies and EU institutions, bodies, offices, and agencies carrying out tasks under Article 37(1)(b) and (c) of the Regulation[29] can obtain access to electronic health data without a data permit under the Data Governance Act.

HDABs and/or data holders will provide access to electronic health data only through a secure processing environment, including technical and organizational measures to restrict access to authorized persons listed in the data permit, and keep identifiable access logs, as well as security and interoperability requirements. For example, data users will only be able to download non-personal electronic health data from the secure processing environment.[30]

HDABs (or the single data provider) and data users will act as joint controllers of electronic health data processed in accordance with data permits.[31]

National contact points for secondary use of electronic health data will be established by Member States and will join the "HealthData@EU" platform to facilitate cross-border access for other participants. Institutions, bodies, offices and agencies across the EU that are involved in research, health policy or analysis will be authorized participants.[32] Third countries or international organizations can also become authorized participants subject to the Commission's assessment of their compliance with the requirements of the "HealthData@EU" platform, the rules of Chapter IV of the Regulation and the existence of equivalent terms and conditions in providing access to data users located

[27] Article 42 of the Regulation.

[28] Article 46(11) of the Regulation.

[29] Supporting public sector bodies, EU institutions, bodies, offices and agencies in carrying out the tasks under their mandate, based on national or EU law.

[30] Article 50 of the Regulation.

[31] Article 51 of the Regulation. The Commission will publish a template for these joint controllers' arrangements.

[32] Article 52 of the Regulation.

in the EU to electronic health data available to their HDABs.[33]

Detailed provisions are made for international transfers of non-personal electronic health data. In particular, certain categories under Article 33 of the Regulation are considered highly sensitive within the meaning of the Data Governance Act due to the risk of re-identification.[34] In addition, data users must take all reasonable technical, legal, and organizational measures to prevent government access to non-personal electronic health data held in the EU, and Article 62 of the Regulation establishes strict conditions to granting access in the case of judgments or decisions from third-country courts, tribunals, or administrative authorities.

Datasets made available by data holders through HDABs can have an EU data quality and utility label that meets certain requirements in terms of data documentation, technical quality, data quality management process, coverage, access and provision, and data enrichments.[35] An EU Datasets Catalogue, linked to national catalogues of datasets, will be established by the Commission under Article 57 of the Regulation.

IV. Additional insights

A new phase of deployment of AI

The EHDS, with health data access bodies as gatekeepers, could herald a new phase of innovation in the deployment of AI systems to large-scale health data to identify new approaches and treatments for diseases.

Employment of AI systems

It is worth noting that secondary use of electronic health data is also allowed for "*training, testing and evaluating of algorithms, including in medical devices, AI systems and digital health applications*" in order to contribute to public health or social security, or to ensure high levels of quality and safety of healthcare, medicinal products or medical devices.[36] As a result, businesses will be able to utilize health data to develop new medical devices or products combined with AI, and to identify new approaches and treatments for diseases, including through precision medicine. In fact, a huge quantity of data is required for the application, testing, and training of AI systems, especially in the case of complex neural networks. In this context, HDABs will support the development of AI systems, including by issuing guidelines and standards for training, testing and validation of AI systems in healthcare.[37]

Regarding the primary use of electronic health data, in addition to the requirements set forth in the Artificial Intelligence Act, when AI systems interoperate with EHR systems, they must also meet the essential interoperability requirements under the Regulation.[38]

Interaction of the Regulation with the GDPR for secondary use of electronic personal health data

Recital 37 of the Regulation specifies the legal basis for secondary use under both Articles 6 and 9 of the GDPR (the requirements of which must be met cumulatively for special categories of personal data, such as health data).

Specifically, the Regulation creates the legal obligation in the sense of Article 6(1)(c) of the GDPR for the disclosure of data by the data holder to HDABs. Moreover, the Regulation assigns tasks in the public interest to the HDABs under Article 6(1)(e) of the GDPR. As for data users that have access to electronic health data for the secondary use of the data for one of the purposes defined in this Regulation, they can demonstrate the existence of a task in the public interest pursuant to Article 6(1)(e) or a legitimate interest under Article 6(1)(f) of the GDPR (explaining the specific legal basis on which it relies as part of the application

[33] Article 52(5) of the Regulation.

[34] Article 61 of the Regulation. Pursuant to Article 5(13) of the Data Governance Act, the Commission will establish special conditions applicable to the transfers of highly sensitive data to third countries.

[35] Article 56 of the Regulation.

[36] Article 34(1)(g) of the Regulation.

[37] Article 37(1)(i) of the Regulation.

[38] Article 14 of the Regulation.

for obtaining the data permit). Where the legal basis under the GDPR is Article 6(1)(e), data users must make reference to another EU or national law (excluding the Regulation) mandating that the data user process personal health data for the performance of its tasks. If the lawful ground is Article 6(1)(f) of the GDPR, the Regulation provides the relevant safeguards, and the data permits issued by the HDABs are administrative decisions defining the conditions for data access.

From the perspective of Article 9 of the GDPR, the Regulation meets the conditions for the processing of electronic health data pursuant to Articles 9(2) (g), (h), (i) or (j) of the GDPR.[39]

Regarding information obligations under Articles 13 and 14 of the GDPR, the Regulation specifies only that HDABs are not required to provide a specific information notice to each natural person concerning the use of their data for projects subject to a data permit, and can provide general public information about all data permits issued.[40] However, the Regulation does not contain provisions regarding the information requirements of data users. In such circumstances, it seems appropriate that they should be able to make use of the exceptions in Article 14(5)(a) or (b) of the GDPR, as the relevant information would have to be provided by the HDABs through the abovementioned reports on the data permits issued or, in any case, that the provision of the information would involve a disproportionate effort.

EDPB and EDPS express concerns

On July 12, 2022, the European Data Protection Board (the "**EDPB**") and the European Data Protection Supervisor (the "**EDPS**") issued a Joint Opinion[41] expressing a range of concerns with the proposed Regulation, including some aspects that may have a weakening effect on data subjects' rights and protections under the GDPR. Although the EDPB and EDPS acknowledged the legislative efforts that have been made to align the proposed Regulation with the GDPR, they called for clarification of the relationship between this innovative legislation and the GDPR and, in particular, for certain changes to the Regulation to address various points of legal uncertainty and inconsistency with the GDPR (for instance, the EDPB and EDPS consider that the definitions of "primary use" and "secondary use" of electronic health data may inherently lead to inconsistency with the GDPR's concept of "further processing of personal data"). They suggest a requirement that electronic health data be stored in the EEA, allowing transfers only pursuant to Chapter V of the GDPR. They express concern about the inclusion of wellness and other digital applications in some aspects of the Regulation, and about the inclusion of wellness and behavior data in the categories of electronic data available for secondary use, as their processing should require individuals' prior consent under the GDPR, and may fall within the scope of the e-Privacy Directive.[42] Finally, the EDPB and the EDPS noted that the purposes for secondary use of health data should have a clear link to public health and/or social security. It is clear that work remains to be done to reconcile legislative uncertainties and ensure a fully functional, GDPR-compliant EHDS scheme.

V. Conclusions

The Commission's proposal has now been transmitted to the Council and is under discussion. After the conclusion of trilogue negotiations, the EHDS will be directly applicable starting twelve months after the entry into force of the Regulation.[43] It will not need to be transposed into national legislation.

However, certain provisions will have different application times. For example, the provisions included

[39] Reasons of substantial public interest (lett. g), preventive or occupational medicine medical diagnosis, provision of health or social care or treatment or the management of health or social care systems, and services from a healthcare professional (lett. h), reasons of public interest in the area of public health (lett. i), and research purposes (lett. j).

[40] Article 38 of the Regulation.

[41] EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space of July 12, 2022, available at https://edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202203_europeanhealthdataspace_en.pdf.

[42] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L 201.

[43] Article 72 of the Regulation.

in Chapter III on EHR systems (implemented pursuant to Article 15(2) of the Regulation) should apply three years after entry into application of the Regulation, as should be the case with the right of access or data portability with respect to medical images, laboratory results, or discharge reports under Article 5(1)(d), (e), and (f) of the Regulation.

In the meantime, businesses operating in the healthcare sector should prepare for the EHDS, evaluating future requirements and opportunities.

…

CLEARY GOTTLIEB