Proposal COM(2022) 197 of 3 May 2022 for a **Regulation** of the European Parliament and of the Council on the **European Health Data Space**.

EU HEALTH DATA SPACE

cep**PolicyBrief** No. 13/2022

LONG VERSION

Authors: Marco Mazzone and Dr. Patrick Stockebrandt | stockebrandt@cep.eu
cep | Kaiser-Joseph-Strasse 266 | 79098 Freiburg | Telephone +49 (0)761 38693-0 | www.cep.eu

A. Key elements of the EU proposal

1 Context and objectives

- In the health sector, in particular, huge gains in value creation and innovation can be achieved through data. It also facilitates truly data-based policy making. However, in almost no other area is data so sensitive. A reasonable compromise therefore needs to be found for the conflict of interests between the increased use of data, which is in the public interest, and the need to protect the individual when using sensitive health data. In this sense, a European health data space is of major importance.

- Expanding the cross-border use of health data has been an EU goal for several years. Recently, the Commission sought to take this further by adopting a recommendation on a European exchange format for electronic health records [(EU) 2019/243; see cep**PolicyBrief** 15/2019].

- The Member States' comprehensive responsibility for healthcare [see cep**Input** 4/2021, pp. 3-6] is the political reason why EU projects in this area have always been formulated as voluntary measures, primarily aimed at the interoperability of national systems [see cep**PolicyBrief** 15/2019]. The lack of interoperability is precisely what makes optimal medical decisions more difficult and causes avoidable costs [Recital 16].

- A central data platform for people to access their own personal electronic health data has been established voluntarily. This used to be called the "eHealth Digital Service Infrastructure" (eHDSI) and now operates under the name of "MyHealth@EU". However, the system so far only supports two services - electronic prescriptions and patient summary - and is only available in ten Member States. [p. 9]

- In addition, the level of digitalisation of health data varies considerably across Member States. In order to support the rights of individuals to access and share their electronic health data, the EU must act to avoid further fragmentation [Recital 20].

- Furthermore, the COVID 19 pandemic has shown the importance of EU-wide public health data [p. 12; see cep**Input** 4/2021, p. 9 et seq.].

- Therefore, the Commission now wants to push ahead with and expedite the EU-wide access to and exchange of electronic health data [hereinafter "health data"] with a Regulation that is fully binding and directly applicable in every Member State. This is intended to create the "European Health Data Space" [hereinafter therefore: EHDS].

- According to the European Data Strategy [COM(2020) 66, see cep**PolicyBrief** 7/2020 and cep**PolicyBrief** 8/2020] the EHDS is one of a series of European Data Spaces that the Commission intends to establish in strategic sectors. This includes EU data spaces on mobility and on financial and energy data [COM(2020) 66, p. 26 et seq.].

- The EHDS is part of comprehensive and coherent data legislation at EU level, such as the General Data Protection Regulation (GDPR), the Data Governance Act [see also cep**PolicyBrief** 6/2021] and the Data Act [see cep**PolicyBrief** 11/2022].

- The EHDS is designed to allow EU citizens to use and control their health data across borders. It will also enable policy makers as well as researchers and innovators to access and use health data whilst safeguarding privacy. [p. 1]

- The EHDS aims to advance the "primary use" and "secondary use" of health data:
  - "Primary use" is the processing of data for the provision of healthcare to natural persons - it therefore concerns personal healthcare [Art. 2 (2) (d); Recital 1].
  - "Secondary use" is processing for other purposes that "benefit society", such as research, policymaking, personalised medicine, official statistics or regulatory activities [Art. 2 (2) (e); Recital 1].

- With its proposal for a Regulation, the Commission is seeking to [Art. 1 (2)]
  - strengthen the rights of the individual;

- lay down rules on national electronic health records systems; and
- establish two separate cross-border data infrastructures: one for primary and one for secondary use of health data.

- The Commission proposal regulates three subject areas:
  - the use of health data for personal healthcare (so-called primary use, Chap. II or Art. 3-13 of the Commission proposal);
  - the systems created for electronic patient records, known as "Electronic Health Records" or EHR (hereinafter therefore: EHR systems) and so-called wellness applications (Chap. III or Art. 14-32 of the Commission proposal); and
  - the use of health data for other purposes (so-called secondary use, Chap. IV or Art. 33-58 of the Commission proposal).

- The Commission's proposal also provides that the rules will take effect twelve months after the adoption of the Regulation. There are, however, special features that will delay the application of certain provisions by a further one to three years. [Art. 72]

2 Health data for personal healthcare (primary use)

2.1 Individual rights

- The EHDS aims to ensure that individuals have access to and control over their health data in the context of their own healthcare [Recital 1].

- "Healthcare" includes all health services provided by "health professionals" to patients to assess, maintain or restore their state of health, including the prescription, dispensation and provision of medicines and medical devices [Art. 2 (1) (b) in conjunction with Art. 3 Patient Mobility Directive (EU) 2011/24].

- The EHDS aims to ensure the rights of individuals, regardless of the Member State in which the health data is processed, the type of healthcare provider or the data sources. It concerns all health data, irrespective of how it was collected or who provided it [Recital 6].

- Basically, individuals have the right,
  - to access their health data from their healthcare immediately, free of charge and in an easily readable, consolidated and accessible format [Art. 3 (1)];
  - to receive an electronic copy of at least their health data in the "priority categories" referred to in Art. 5 of the Commission proposal [Art. 3 (2)].

- The "priority categories" include [Art. 5 (1) in conjunction with Annex I]:
  - Patient summaries; these contain the individual's most important clinical data, e.g. information on
    - allergies;
    - vaccinations;
    - medical devices and implants;
    - current and previous medications; and
    - other data provided by the patient.
  - electronic prescriptions (e-prescriptions);
  - medical images and image reports;
  - laboratory results;
  - discharge reports.

- The Commission will have the power to amend the list of "priority categories". It will also be able to extend, modify or remove the main characteristics of those categories and indicate a deferred application date [Art. 5 (2)].

- Member States may require that non-electronic health data, recorded prior to application of the Regulation, be made available in electronic format [Art. 3 (4)].

- In order for individuals to exercise their rights, Member States have to establish health data "access services" - i.e. online services such as a portal or an app [Art. 3 (5) (a); Art. 2 (2) (i)]. Member States must also allow an authorised representative to access the individual's data [Art. 3 (5) (b)].

- Individuals also have the right,
  - to independently insert health data into their own electronic health records, and this data will then be highlighted [Art. 3 (6)];
  - to have their data rectified, and Member States must ensure that this can be easily requested online [Art. 3 (7)];
  - require entities in the health or care sector that hold health data - e.g. doctors, hospitals, etc. - to give access to the data or transmit it to other appropriate entities, immediately, free of charge and without hindrance in each case [Art. 3 (8)];
  - to restrict access by third parties, e.g. doctors, to all or part of their health data [Art. 3 (9)];
  - to obtain information, immediately and free of charge, about the persons - e.g. the doctors or pharmacists - who have accessed their health data in the context of healthcare [Art. 3 (10)].

2.2 Access to health data by health professionals

- "Health professionals", e.g. doctors, nurses, dentists, midwives or pharmacists [see Art. 2 (1) (b) in conjunction with Art. 3 Patient Mobility Directive (EU) 2011/24], have access to the existing data of the person under their treatment [Art. 4 (1) (a)]. They, in turn, can - and should - update the existing data with the data that is then generated [Art. 4 (1) (b)].

- Member States may stipulate which categories of health data are required by different health professions [Art. 4 (2)]. However, they must ensure that access is granted to at least the "priority categories" under Art. 5 of the Commission proposal [Art. 4 (3)].

- Individuals can restrict access to their health data but hospitals, doctors, nurses, etc. can still get access to restricted health data in case of "vital interests". The person concerned must then be informed of this. [Art. 4 (4)]

2.3 National "digital health authority" and "MyHealth@EU"

- Each Member State must designate a "digital health authority" responsible for the implementation and enforcement of the rules at national level [Art. 10 (1)].

- The tasks of the "digital health authorities" include: [Art. 10 (2)]
  - implementation of the rights and obligations provided for in Chapters II and III of the Commission proposal by adopting national, regional or local technical solutions [(a)];
  - implementation, at national level, of the European electronic health record exchange format and its further development at EU level [(g) and (h)];
  - where applicable, market surveillance activities in accordance with Art. 28 of the Commission proposal [(i)];
  - the provision of telemedicine services in compliance with national law [(k)]. The following applies in this regard: If a Member State accepts telemedicine services in its health system, it must also accept the same type of services from other EU countries [Art. 8];
  - promoting the availability of telemedicine services and ensuring their ease of use and accessibility for all [(k), Recital 9].

- A central data platform, enabling the use of health data for one's own healthcare, has already been established voluntarily and is now called "MyHealth@EU". It supports and facilitates the exchange of health data between Member States [Art. 12 (1)].

- Member States must designate one national contact point for this, which will ensure the connection to all other contact points as well as to "MyHealth@EU" [Art. 12 (2)].

- The contact points will enable the exchange of health data based on the European electronic health record exchange format [Art. 12 (3)].

- The Commission is empowered to further develop "MyHealth@EU", e.g. with regard to technical development, security, confidentiality and protection of health data [Art. 12 (4)].

- Member States must ensure that
  - all healthcare providers are connected to their national contact points and that the two-way exchange of health data is enabled [Art. 12 (5)];
  - their pharmacies (both on-site and mail-order) can dispense e-prescriptions issued in the EU and transmitted to them via "MyHealth@EU" [Art. 12 (6)].

- "MyHealth@EU" will also allow Member States to provide supplementary services, e.g. to facilitate telemedicine and mobile healthcare or to access translated health data [Art. 13 (1)].

- The Commission and the Member States will seek to make MyHealth@EU interoperable with the technological systems established at international level for the exchange of health data [Art. 13 (3)].

3 Requirements for manufacturers of EHR systems and "market surveillance"

- The Commission proposal establishes a plethora of requirements which the systems created for "Electronic Health Records", [see Art. 2 (2) (m + n), hereinafter: EHR systems] must meet.

- An EHR system is any appliance or software intended by the manufacturer for storing, intermediating, importing, exporting, converting, editing or viewing electronic health records [Art. 2 (2) (n)].

- In addition, manufacturers of EHR systems in particular have to comply with a large number of further obligations [most notably Art. 17 in conjunction with Annex II].

- Member States are responsible for designating market surveillance authorities to ensure compliance with the requirements for EHR systems [Art. 28 et seq.] Member States are also responsible for penalties [Art. 69].

3.1 Requirements for EHR systems, further obligations of manufacturers, penalties

- The requirements are aimed in particular at manufacturers of EHR systems. They include: [Art. 17 in conjunction with Annex II]
  - General requirements, e.g. that [No. 1 of Annex II]
    - EHR systems be designed and manufactured in such a way as to uphold the rights of the individual;
    - EHR systems that are operated with other products - including medical devices - are reliable, secure and allow for the exchange of health data.
  - Requirements for interoperability, e.g. that [No. 2 of Annex II]
    - EHR systems allow health data to be shared in an interoperable format so as to ensure that exchange can take place between all health professionals, in particular between doctors, between doctors and other bodies in the health system, and even between doctors and online portals for patients;
    - EHR systems are interoperable and compatible with the European infrastructure for cross-border sharing of health data.
  - Requirements for security, e.g. that [No. 3 of Annex II]
    - EHR systems ensure secure processing of health data and prevent unauthorised access;
    - EHR systems, to the extent that they are designed for use by health professionals, ensure reliable identification and authentication;
    - EHR systems provide sufficient logging mechanisms so that, in particular, the individual, the data category(ies) and the date and time of every access are recorded;
    - EHR systems allow individuals to restrict access to their health data by health professionals, e.g. doctors - although access is still allowed in emergencies but must be strictly logged.

- The Commission is empowered to lay down the requirements for EHR systems in the form of "common specifications" - including a time limit for their implementation - by means of implementing acts [Art. 23 (1)].

- Manufacturers are responsible for the EU declaration of conformity and the affixing of the CE marking [Art. 17 (1) (d) + (e); Art. 26; Art. 27].
  - The EU declaration of conformity shows that the requirements for the EHR system have been fulfilled. By issuing them, the manufacturer assumes responsibility for the conformity of the EHR system [Art. 26].
  - The CE marking certifies the conformity of the product with the requirements of the relevant EU provisions which require it to be affixed [see Art. 27 (1) and Art. 27 (2) in conjunction with Art. 30 Regulation (EC) 765/2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products].

- The Commission must establish and maintain a public database containing information on EHR systems for which an EU declaration of conformity has been issued [Art. 32 (1)]. Before placing an EHR system on the market or putting it into service, the manufacturer must register it in the database [Art. 32 (2)].

- Insofar as an EHR system does not comply, or has ceased to comply, with the requirements ["non-conformity"], the manufacturer must
  - take any necessary corrective action, without undue delay, recall the system or withdraw it from the market [Art. 17 (1) (g)]; and
  - inform the market surveillance authorities of the Member States, in which the EHR system is available, about the non-conformity and about corrective actions already taken [Art. 17 (1) (i)].

- EHR system manufacturers must also report, to the market surveillance authorities of the Member States concerned, any "serious incident" involving an EHR system, and the corrective actions taken or envisaged in this respect [Art. 29 (4)].

- A "serious incident" is any malfunction or deterioration in the characteristics or performance of an EHR system made available on the market which directly or indirectly leads, might have led or might lead to any of the following consequences: [Art. 2 (2) (q)]
  - the death of a person or serious damage to a person’s health; or
  - a serious disruption to the management and operation of critical infrastructure in the health sector.

- Member States are responsible for adopting provisions on penalties. The penalties must be "effective, proportionate and dissuasive". [Art. 69, Recital 70]

3.2 Market surveillance of EHR systems by Member States

- Member States designate a market surveillance authority and provide it with the necessary powers, resources, equipment and knowledge [Art. 28 (2)].

- These authorities will report regularly to the Commission on the results of their market surveillance [Art. 28 (4)]. They cooperate with each other and with the Commission, which will organise the exchange of information necessary for this purpose [Art. 28 (5)].

- Where a market surveillance authority finds that an EHR system presents a risk, in particular to the health or safety of persons, it must
  - require the manufacturers of the EHR system to remove the risks, withdraw the EHR system from the market or recall it [Art. 29 (1)];
  - inform both the Commission and the other market surveillance authorities immediately thereof [Art. 29 (3)].

- In the event of a "serious incident", the market surveillance authorities must inform the other market surveillance authorities, without delay, of the incident and of the corrective action already taken or envisaged by the manufacturer, or required of it [Art. 29 (5)].

- In particular, if an EHR system is not (or no longer) in conformity with the requirements, the EU declaration of conformity has not been drawn up correctly or at all, or the CE marking has not been affixed or has not been affixed in accordance with the regulations, the market surveillance authority will request the manufacturer to remedy this [Art. 30 (1)].

- In the event of a failure to comply, the Member State will take all appropriate measures to restrict or prohibit the EHR system from being placed on the market or to ensure that it is recalled or withdrawn from the market [Art. 30 (2)].

4 "Wellness applications" - devices or software for maintaining a healthy lifestyle

- "Wellness applications" are devices or software, e.g. fitness watches or fitness apps, with which individuals can generate health data outside institutionalised healthcare, e.g. in order to maintain a healthy lifestyle [see accordingly Art. 2 (2) (o)].

- Insofar as the manufacturer of a wellness application claims that it is interoperable with an EHR system - i.e. that the health data generated by the application can be transferred to the electronic patient record, for example - it can be given a label to that effect ("label") [Art. 31 (1)].

- The label is issued by the manufacturer of the wellness application and indicates that it is interoperable with an EHR system and meets the essential requirements under Art. 23 and Annex II of the Commission proposal [Recital 35, Art. 31 (1)]. The period of validity must not exceed five years [Art. 31 (5)].

- The Commission will establish and maintain a public database containing information on wellness applications for which a label has been issued [Art. 32 (1)]. Before placing a wellness application on the market or putting it into service, the manufacturer must register it in the database [Art. 32 (2)].

- Due to the large number of wellness applications and the often limited relevance for health purposes of the health data they generate, the Commission takes the view that a certification system would be disproportionate. It therefore considers a voluntary labelling scheme to be an appropriate means for making compliance with the requirements transparent for users [recital 35].

- Market surveillance authorities must verify that wellness applications comply with the requirements laid down in Annex II of the Commission proposal [Art. 31 (7)].

5 Health data for other purposes (secondary use)

5.1 Basic aspects

- The proposed Regulation creates the legal basis for the secondary use of health data and lays down safeguards for the processing of health data [Recital 37].

- "Secondary use" is the processing of health data for purposes other than the actual healthcare of the individual; such as policy making, regulation, research and development, personalised medicine or official statistics [Art. 2 (2) (e); Recital 1].

- The provision of health data is intended to support in particular: [Recital 41; Art. 34]
  - the performance of public tasks, such as health surveillance, planning and reporting, as well as health policy making;
  - scientific research (including private research), development and innovation as well as the production of goods and services for the health or care sectors.

- Health data already exist and is being collected by healthcare providers, professional associations, public associations, regulators, research institutions, insurers, etc. in the course of their activities [Recital 38].

- However, much of the existing health data cannot be used for anything other than the original purpose for which it was collected. This limits the potential use for research, innovation, policymaking, regulation, patient safety or personalised medicine. [Recital 38]

- The proposed Regulation establishes the legal obligation of the "data holder" to disclose health data to "health data access bodies" [Art. 33, Art. 36; Recital 37]. This does not apply to enterprises that employ fewer than 10 persons and whose annual turnover or annual balance sheet does not exceed two million euros - so-called micro-enterprises [Art. 33 (2) in conjunction with Art. 2 (3) of the Annex to Commission Recommendation 2003/361/EC].

- The term "data holder" is broadly defined in this case. It covers, on the one hand, EU institutions, EU bodies and other EU agencies that are authorised or obliged to process health data and, on the other hand, public and private actors that process the health data covered under Art. 33 ("minimum categories"), namely [see accordingly, Art. 2 (2) (y); Recital 40]
  - health or care providers,
  - organisations, professional associations and other institutions, as well as
  - research institutions in the health sector.

- The "health data access bodies" are designated by the Member States. Among other things, they are responsible for ensuring access to health data, processing data access applications and issuing data permits. [Art. 36, Art. 37, Art. 45]

- Where a data controller is obliged to make health data available, it must cooperate constructively with the access bodies ("in good faith") [see accordingly Art. 41 (1)].

- In principle, any natural or legal person may submit a data access application for the "permitted purposes" [see below, section 5.2.2] [Art. 45 (1)].

- Due to the special importance of health data, it is always provided in an anonymised format. If the purpose of processing cannot be achieved by this, the health data may be provided in a pseudonymised format. The applicant will justify why this type of data is necessary [Art. 44 (2) and (3); Recital 49].

- Data users are not allowed to recreate the identity of pseudonymised health data. Appropriate penalties fall within the remit of the Member States [see accordingly Art. 44 (3) and Recital 49].

- Despite state-of-the-art anonymisation techniques, an ability to reconstruct the identity of a natural person cannot be ruled out. This is principally the case for rare diseases due to the limited number of cases - but also in other cases, in particular by linking health data with other information or through new technological methods [Recital 64].

5.2 Data categories and permitted and non-permitted secondary use

5.2.1 Minimum categories of electronic data for secondary use

- Data holders must make available the following categories ("minimum categories") of electronic data [Art. 33 (1)]:
  - electronic health records [(a)];
  - data impacting on health, including social, environmental and behavioural determinants of health, e.g. substance use, homelessness or professional status [(b) and Recital 39];
  - relevant pathogen genomic data, impacting on human health [(c)];
  - health-related administrative data, including claims and reimbursement data [(d)];
  - human genetic and genomic data [(e)];
  - person-generated health data, including from medical devices and wellness applications [(f)];
  - health data from population wide registries [(h)];
  - health data from medical registries for specific diseases [(i)];
  - health data from clinical trials [(j)];
  - health data from medical devices and from registries for medicinal products and medical devices [(k)];

  - health-related electronic data, including on insurance status, professional status, education, lifestyle and wellness, and behaviour [(n)].

- The Commission is empowered to amend the list of minimum categories [Art. 33 (7)].

- Health data containing protected intellectual property and trade secrets of private companies will also be made available for secondary use. In this regard, "all necessary measures" must be taken to protect intellectual property rights and the confidentiality of trade secrets [Art. 33 (4)].

5.2.2 Permitted and non-permitted secondary use

- Health data may only be processed for secondary use if the applicant uses the processing for one of the purposes specified by law. Thus, the secondary use of health data is permitted [Art. 34 (1)]
  - in the public interest, particularly in the field of public and occupational health - e.g. to protect against serious cross-border health threats or for public health surveillance [(a); see also Art. 34 (2)];
  - to support public sector bodies or e.g. EU institutions in the health or care sector so that they can carry out their tasks as defined in their mandates [(b); see also Art. 34 (2)];
  - for the production of official statistics on the health and care sectors [(c); see also Art. 34 (2)];
  - for scientific research in the health or care sector [(e)];
  - for development and innovation activities for products or services that contribute to public health or social security, or for ensuring high standards of quality and safety of healthcare, medicinal products or medical devices [(f)];
  - for the evaluation and improvement of algorithms, including in medical devices or digital health applications, e.g. to ensure high levels of quality and safety of healthcare, medicinal products or medical devices, or to contribute to public health [(g)];
  - for the provision of personalised healthcare in which the health status of the individual is assessed, maintained or restored on the basis of the health data of other individuals [(h)].

- Any attempt to use health data for measures detrimental to the person concerned, to increase insurance premiums, to advertise products or treatments or to develop harmful products should be prohibited [Recital 41]. It is therefore prohibited to use health data for secondary use for the following purposes [Art. 35]:
  - taking decisions detrimental to a natural person based on his or her health data [(a)];
  - taking decisions concerning a natural person or groups of natural persons in order to exclude them from the possibility of concluding an insurance contract or to modify their contributions and insurance premiums [(b)];
  - advertising and marketing activities targeting health professionals, healthcare organisations or natural persons [(c)];
  - disclosure (providing access to, or otherwise making available) of the health data to third parties not specified in the relevant data permit [see below, section 5.6] [(d)];
  - development of harmful products and services, e.g. illicit drugs, alcoholic beverages, tobacco products or goods/services that are contrary to public order or morality [(e)].

5.3 Health data access bodies

- Member States must designate one or more "health data access bodies" [hereinafter: access bodies] that grant access to health data for secondary use [Art. 36 (1)].

- The access bodies carry out, inter alia, the following tasks [Art. 37]:
  - deciding on data access applications [Art. 45] and data requests [Art. 47] [(a)];
  - supporting public authorities [(b)] and EU institutions, bodies, offices and agencies in the carrying out their tasks [(c)];
  - safeguarding the confidentiality of trade secrets and intellectual property rights [(f)];
  - gathering and compiling health data from various data holders and making the data available to the data user in a secure processing environment [Art. 50] [(g)];

- supporting the development of artificial intelligence systems [hereinafter: AI systems] and the training, testing and validation of AI systems [(i)];
- ensuring cross-border access to health data for secondary use via "HealthData@EU" [(o)];
- the publication of various information on its website, in particular all data permits, requests and applications as well as penalties imposed pursuant to Art. 43 [(q)].

- The Commission is empowered to amend the list of tasks [Art. 37 (4)].

- Access bodies also have a duty to provide information about the conditions under which health data is made available for secondary use, in a publicly accessible and easily searchable manner [Art. 38 (1)].

- The access bodies must continue to publish an annual report [Art. 39 (1)]. This includes, among other things, information about:
  - the type of applicants, the number of data permits granted and refused, and the purposes of access [(a)];
  - the fulfilment of commitments by data users and data holders and on penalties imposed [(c)];
  - the requests from natural persons on the exercise their data protection rights [(f)];
  - the revenue from data permits and data requests [(i)];
  - the satisfaction of the applicants [(j)];
  - the average number of days between application and access to data [(k)].

- The access bodies monitor and supervise compliance with the requirements imposed on data users and data holders [Art. 43 (1)].

- In the event of infringements, the access bodies may impose various penalties [Art. 43], for which the Commission may establish guidelines [Art. 43 (10)]. With respect to the data user, access bodies may, for example, revoke the data permit, terminate the processing operation and exclude a data user from access to the EHDS for a period of up to five years [see especially Art. 43 (4) and (5)]. The possibility of a judicial remedy must be guaranteed [Art. 43 (9)].

- The access bodies must ensure data minimisation and purpose limitation [Art. 44]:
  - They must ensure that the data user only has access to the health data that is requested and that is relevant for the purpose and to that extent is covered by the data permit [Art. 44 (1)].
  - They must provide the health data in an anonymised format if this can achieve the stated purposes [Art. 44 (2)].
  - If the purposes stated by the data user cannot be achieved with anonymised data, the access body must provide it in a pseudonymised format. Only the access body has access to the information necessary to reverse the pseudonymisation. Data users are not allowed to re-identify the pseudonymised health data, otherwise they will face "appropriate penalties" [Art. 44 (3)].

- The access bodies are responsible for a secure processing environment for health data [Art. 50 (1)]. They must ensure that health data can be uploaded by data holders and accessed by the data user, whilst only non-personal health data can be downloaded from the secure processing environment [Art. 50 (2)].

- In this regard, they must ensure, inter alia, that [Art. 50 (1)]
  - only those authorised under the data permit have access to the processing environment [(a)];
  - the risk of unauthorised access to health data is minimised by state-of-the-art technological means [(b)];
  - the ability to amend and delete health data is limited to a small number of identifiable individuals [(c)].

5.4 Obligations of data holders

- The data holder provides the access body with a general description of its dataset [Art. 41 (2)]. This requires information on the source, scope, main characteristics and nature of the health data and the conditions for making it available [see Art. 55 (1)].

- Data holders must provide the access body with the health data within two months of receiving the access body's request. The access body may extend this period by two months in exceptional cases [Art. 41 (4)].

- Where data holders hold non-personal health data, they must ensure that access to it is based on trusted and open databases to ensure unrestricted access for all users and electronic archiving of the data [Art. 41 (6)].

5.5 Fees

- Access bodies and data holders may charge fees for the provision of health data. These include all significant costs incurred in connection with the provision of the health data [Art. 42 (1)].

- If the data is not held by the access body or a public body, additional fees may apply for the specific collection of health data. The data holder receives that part of the additional fees related to its costs [Art. 42 (2)].

- The fees must be presented transparently and must be proportionate to the cost of collecting and providing the health data, objectively justified and must not restrict competition. The fees are reduced in certain cases, e.g. for small and medium-sized enterprises ("SMEs") or public bodies, in proportion to their size or budget [Art. 42 (4)].

- If no agreement is reached between the data holder and the data user within one month of the data permit being granted, the access body may set the fees in proportion to the cost of providing the health data. Where the fee assessment is disputed, there is access to dispute settlement bodies [Art. 42 (5)].

- The Commission can lay down principles and rules for the fee policies and fee structures by means of implementing acts [Art. 42 (6)].

5.6 Applications for data access and data permits

- Any natural or legal person may, in principle, submit a data access application [Art. 45 (1)].

- In doing so, the applicant must explain the purposes for which he/she intends to use the health data and whether he/she requires it in anonymised or pseudonymised format [Art. 45 (2) (a), (c) and (d)].

- If data is requested in pseudonymised form, the applicant must give the reasons for this. An ethical assessment may also be required subsequently based on national law [Art. 45 (2) (d), Art. 45 (4) and Recital 50].

- The access bodies must fully assess the applications and issue a data permit if all necessary requirements are met, otherwise the application will be refused [Art. 46 (1) and (2)]. If a data permit is refused, the applicant must be provided with a justification [Art. 46 (5)].

- Due to limited resources, access bodies may set rules that prioritise, for example, public institutions over private bodies. However, within a prioritisation category, institutions located in their own country should not be given preference over those located in other Member States [Recital 51].

- The decision on a data permit must be taken within two months of receiving the data access application. This time limit may be extended by a further two months. If an access body fails to reach a decision during this time limit, the data permit is deemed to have been issued. [Art. 46 (3)]

- The data permit gives the applicant the right to access and process the health data [Art. 46 (7)].

- A data permit is granted for the period necessary to fulfil the purposes - but not exceeding five years. In justified cases, a one-time extension of up to five years is possible [Art. 46 (9)].

- Data users are obliged to publish their results or output based on the health data in anonymised form [Art. 46 (11)].

- The Commission is empowered to amend the aspects to be covered in a data permit [Art. 46 (8)].

5.7 "HealthData@EU"

- Member States and the Commission must establish cross-border infrastructure for the EU-wide secondary use of health data ("HealthData@EU") to promote and facilitate EU-wide access to such data. By doing so, they will connect up the "national contact points for secondary use of electronic health data" [see Art. 2 (2) (u); hereinafter: national contact point] of all the Member States and all other authorised participants [Art. 52 (8)].

- Each Member State will designate a national contact point responsible for making electronic health data available across borders. The task can also be assigned to the "health data access bodies" [see above, section 5.3]. The national contact points are "authorised participants" of "HealthData@EU". [Art. 52 (1) and (2)]

- Other authorised participants of "HealthData@EU" are:
  - EU institutions, bodies and agencies involved in research, health policy or analysis, e.g. the EU Centre for Disease Prevention and Control (ECDC; see also on this cep**PolicyBrief** 17/2021) [Art. 52 (3)];
  - Health-related research infrastructures or similar structures whose work is based on EU law - e.g. a European Research Infrastructure Consortium ("ERIC") under the relevant Council Regulation [(EC) 723/2009] - and the use of the health data is conducive to research, policy-making, statistics or patient safety [Art. 52 (4); Recital 55];
  - Third countries or international organisations, provided that they comply with the rules accompanying the EHDS and grant EU-based data users access to health data held by their access bodies, under equivalent terms and conditions [Art. 52 (5)].

- The Commission is responsible for the creation and operation of a core platform for "HealthData@EU" which will provide IT services to connect the access bodies with each other [Art. 52 (9)].

- In particular, the Commission is empowered to establish and amend the categories of "authorised participants" [Art. 52 (7)] and the requirements, technical specifications and IT architecture, etc. of "HealthData@EU" [Art. 52 (13)].

B. Legal and political context

1 Legislative Procedure

3 May 2022	Adoption by the Commission
Open	Adoption by the European Parliament and the Council, publication in the Official Journal of the European Union, entry into force

2 Options for Influencing the Political Process

Directorates General:	DG Health and Food Safety
Committees of the European Parliament:	Civil Liberties, Justice and Home Affairs [LIBE] and, Environment, Public Health and Food Safety [ENVI] (joint lead), Internal Market and Consumer Protection [IMCO] and Industry, Research and Energy [ITRE]; Rapporteur TBA
Federal Ministries:	Health (leading)
Committees of the German Bundestag:	TBA
Decision-making mode in the Council:	Qualified majority (acceptance by 55% of Member States which make up 65% of the EU population)

3 Formalities

Legal competence:	Art. 16 TFEU (Data Protection), Art. 114 TFEU (Internal Market)

Form of legislative competence:	Shared competence (Art. 4 (2) TFEU)
Legislative Procedure:	Art. 294 TFEU (ordinary legislative procedure)

C. Assessment

1 Economic Impact Assessment

1.1 Basic aspects

According to Art. 4 (15) GDPR, health data is "[...] personal data related to the physical or mental health of a natural person [...] which reveals information about his or her health status". Furthermore, it falls under particularly sensitive categories of personal data pursuant to Art. 9 GDPR, along with personal data revealing, for example, ethnic origin, political opinions, religious or philosophical beliefs. Accordingly, processing this data is generally prohibited but may be permitted in individual cases (prohibited unless authorised). The cases referred to in Art. 9 (2) GDPR regarding health data are limited in form but broad in content.[1]

Thus, health data is classed as data that is particularly sensitive and worthy of protection and which can also affect the privacy of the respective natural persons and therefore their human dignity.[2] The Commission proposal therefore correctly provides for an explicit ban on the processing of health data in the area of secondary use for specific purposes, such as the adjustment of insurance premiums. This is also necessary to increase the confidence of EU citizens in the EHDS, which is essential for its functioning.

Member States are largely responsible for the healthcare sector. In the past, this has led to the EU pushing for the cross-border use of health data mainly by way of voluntary measures. Now, the COVID 19 pandemic has revealed the importance of data sharing and the use of health data. This will not only help to better identify potential serious cross-border health threats, but also improve the response to such hazardous situations. Thus, the EHDS - in addition to other measures, e.g. the creation of the health authority HERA [see cep**Input** 8/2022] and the new competences for the European Medicines Agency EMA [see cep**PolicyBrief** 12/2021] - will be able to contribute to better prevention and more efficient crisis management in the future.

The previously voluntary EU projects on the cross-border use of health data were mainly aimed at ensuring the interoperability of national systems. There has been progress in this regard but, precisely because of the voluntary nature of the process - as regards the EU as a whole -, implementation has been inadequate. The Commission now wants to remedy this situation with the more stringent instrument of a Regulation. It will also be easier for EU citizens to make use of medical services in other EU countries, which in terms of the freedom of movement and overall high level of mobility within the EU, will be a positive development. This is particularly important in border regions, where medical services are regularly used across borders - especially in emergencies, e.g. when hospitals in a particular Member State have no available capacity. In future, doctors and other health professionals will be able to access translated electronic patient records, for example. This will facilitate safer and more efficient healthcare. In addition, non-interoperable systems can give rise to avoidable costs, e.g. due to unnecessary duplication of examinations[3] or incorrect medication [see also cep**PolicyBrief** 15/2019]. Overall, the EHDS can help to save unnecessary costs and generate efficiency gains.

1.2 Positive impact of an EHDS: Concrete examples of use

The EHDS may help with progress in relation to so-called rare diseases. Rare diseases only affect a relatively small number of people[4] and are often associated with chronic or life-threatening conditions. A large proportion of them - up to 80 percent - are genetic in the broadest sense and often incurable. There are more than 6,000 rare diseases and around 30 million people in Europe suffer from one of these diseases.[5] As relatively few people are affected by rare diseases, there is a lack of incentive to conduct research and develop appropriate medicines. The background to this is that, generally, not even research and development costs are amortisable in this regard.

---

1 Petri (2022), Die primäre und sekundäre Nutzung elektronischer Gesundheitsdaten. Zum Vorschlag der EU-Kommission für einen Europäischen Gesundheitsdatenraum, p. 414.
2 Ibid., p. 413.
3 What has still not be ruled out, however, is the duplication of examinations due to monetary incentives.
4 A disease is considered rare if it affects a maximum of 5 in 10,000 people (see Federal Ministry of Health (2022), Seltene Krankheiten.
5 Federal Ministry of Health (2022), Seltene Krankheiten.

In addition, there is a need for improvement in the detection/screening of rare diseases[6] which differs significantly from one Member State to another.[7] However, the earlier a rare disease is detected, the more chance there is of influencing the progress of the disease in the patient's favour.[8] The EHDS will facilitate better collection, sharing and analysis of health data, especially relating to rare diseases. There is a legitimate hope for better understanding of rare diseases and the advancement of drug development.

Another important health policy project in the EU is the fight against resistance to antibiotics, which has developed in humans and animals due to the overuse of antibiotics in agriculture, extensive use in human medicine and improper disposal in the environment.[9] As a result, antibiotics work less effectively or not at all in the treatment of infectious diseases, which can have life-threatening consequences.[10] There is an overall shortage of new and effective antibiotics, as their development is less economically profitable than, for example, the development of cancer drugs. The World Health Organisation (WHO) regards antimicrobial resistance as one of the top ten threats to public health and has coined the term "silent pandemic" due to the deaths attributable to multi-resistant bacteria. In the EU, the death toll from multi-resistant germs is estimated at around 33,000 a year.[11] It has also been forecast that, if no action is taken, up to 10 million people a year could die worldwide by 2050, due to antimicrobial resistance. The economic costs associated with such a crisis would be similar to those caused by the global financial crisis of 2008-2009.[12] Overall, the EHDS may help to facilitate a better understanding of antimicrobial resistance by allowing health data to be shared. This could contribute to the development of new and more effective antibiotics that could save many lives, including outside the EU.

1.3 Impact on digitalisation and competition

Digitalisation

The digitalisation of healthcare in the Member States has progressed at very different rates. Finland and Estonia can be described as pioneers among the EU countries. Other countries, such as Germany, are struggling to make progress with digitalisation. So far, the central data platform enabling people to use personal electronic health data for their own healthcare, which up to now has been established voluntarily, has not had a resounding success - as regards the entire EU. The current system - now called "MyHealth@EU" - supports only two services, e-prescriptions and patient summaries, and is mainly used by the pioneers - such as Finland and Estonia. Countries like Germany are clearly lagging behind. In Germany, for example, important projects such as the electronic sick note or the e-prescription have not yet been fully and comprehensively implemented due to a wide variety of stakeholder interests and technical problems. The EHDS is important in order to prevent further fragmentation and, in particular, to hold Member States such as Germany to account so that the desired and very important digitalisation of national health systems can be expedited.

As regards the primary use of health data, e-prescriptions will be redeemable across borders in all on-site and mail-order pharmacies through "MyHealth@EU". This promotes competition between the different pharmacies, which in turn can lead to lower prices and more attractive conditions for EU citizens. It also promotes the mobility and free movement of EU citizens, who can thus redeem their prescriptions quite easily throughout the EU.

Competition

The market for digital health applications is still in its infancy - from a Europe-wide perspective. The creation of a single market for health data may spark competition and open up potential for growth. The so-called "big tech companies", in particular, have recognised this. So far, they are mainly involved in the areas of apps, wearables,

---

6 Ibid.

7 The EU could, for example, contribute to better recognition of rare diseases across the EU with targeted support or exchange of best practices.

8 Euractiv (2022), Newborn screening is vital but differs from one European country to another.

9 See Brombach / Sattelberger (2018), Antimicrobial Resistance, cep**PolicyBrief** 01/2018 and Rothe / Stockebrandt (2020), Pharmaceuticals in the Environment, cep**PolicyBrief** 02/2020.

10 Background: Active pharmaceutical ingredients are mainly produced in Asia, especially in India and China. This is problematic given existing bottlenecks and supply chains that are under strain. In order, above all, to reduce dependencies, the Commission is proposing to bring parts of the production back to Europe; see euractiv.de (2020), Commission aims to "bring back"medicine production to Europe and Handelsblatt (2022), Pharmabranche warnt vor Abhängigkeit aus Fernost - EU will mit neuer Arzneistrategie reagieren. These dependencies also include a geopolitical component: see the comments made by Ulrike Holzgrabe, professor of pharmacy at the University of Würzburg: "The Chinese don't need a nuclear bomb. They can simply stop supplying antibiotics [...], then Europe will collapse of its own accord"; Pharmazeutische Zeitung (2020), Produktion zurück nach Europa holen.

11 Europe.Table (2022), Antibiotic resistance: EU action needed more than ever.

12 WHO (2019), New report calls for urgent action to avert antimicrobial resistance crisis.

online pharmacies and clinical trials.[13] It is also apparent that companies such as Google are selectively acquiring (emerging) companies in order to either eliminate potential competitors and/or take over their technology and expertise. A prominent example is Google's acquisition of Fitbit, a fitness tracker manufacturer. Fitbit is particularly well known for its wellness applications.[14] The US tech majors already have overwhelming market power in various segments. Thus, it should be noted that tech companies could increase their respective market power by accessing health data for secondary use. Antitrust considerations should also, therefore, be taken into account when deciding on access to health data. In the case of public, private or non-profit institutions that do not (yet) have such a high degree of market power, on the other hand, antitrust considerations should accordingly have no consequences.

In addition to innovations in the (digital) health sector, the EHDS also promotes competition as a whole and in this respect should receive a favourable assessment. Most notably, it may improve healthcare for individuals and combat cross-border health threats.

1.4 Control over health data and “opt-in” versus “opt-out”

Control over health data

A primary concern of the EHDS is to give EU citizens sovereignty over their health data. They should be enabled to access and control this data.[15] The fact that EU citizens will in future have the right to access health data arising from their healthcare, immediately, free of charge and in an accessible format, is a positive development. Currently, health data is generally unsystematic and scattered among the various health professionals or healthcare providers. Access is extremely difficult in many Member States.

Furthermore, the suggestion on primary use also provides for effective control over health data. Thus, individuals can deny third parties, e.g. doctors, access to all or some of their health data. In order to ensure establish confidence in the EHDS among EU citizens, the draft correctly envisages strict requirements for the respective national systems (EHR systems). Thus, identification and authentication are required every time the system is accessed. In addition, every access to the relevant patient records is logged.

However, the same level of control cannot be said to exist over the secondary use of health data. This is because there is no possibility of an “opt-out” out when it comes, for example, to the secondary use of data contained in the electronic health records of EU citizens. Even if secondary use occurs for worthwhile purposes, such as health research, it must be clear that there is then no longer any model for consent. EU citizens should, nevertheless, have the freedom of choice.

"Opt-in" versus "opt-out": Context and discussion

This could be realised in one of two ways: On the one hand, by way of consent ("opt-in"). On the other hand, by way of an objection ("opt-out").

Context: A discussion regarding the advantages and disadvantages of opt-in and opt-out models is being conducted in many different areas of health policy. For example: In order to promote the (actual) use of electronic health records (EHRs) in Germany, the coalition government, made up of the SPD, Greens and FDP, has provided for[16] a change from "opt-in" to "opt-out” in the coalition agreement. This comes against the backdrop that use of the EHR in Germany so far remains vanishingly small.[17] The exact design - e.g. whether the EHR will start off "empty" or whether it will already contain (existing) health data - remains unclear.[18] However, it is likely that the changeover will see a significant increase in the number of EHR users as such "nudging”[19] may break through the status quo. This has been seen in other Member States such as Austria, Estonia and some regions of Spain that have already implemented opt-out models. In Austria, for example, only 3 per cent of

---

13 Brainwave hub (2022), BIG TECH MEETS HEALTHCARE. Die Digital Health Strategien von Amazon, Apple, Google und Microsoft, p. 1.

14 The takeover of Fitbit by Google was only approved by the European Commission subject to conditions. For more details see European Commission 2020, Case M.9660 - GOOGLE/FITBIT.

15 This will certainly also change the doctor-patient relationship.

16 Coalition agreement between SPD, Bündnis 90/Die Grünen and FDP (2021), Mehr Fortschritt wagen. Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit, p. 83.

17 Bertelsmann Stiftung (2022), Opt-out bei der Patientenakte. Die Möglichkeiten der Digitalisierung ausschöpfen, p. 2.

18 See also ibid., p. 2 et seq.

19 “Nudging" refers to the idea of prodding people to make certain decisions (deemed correct) on a one-time or permanent basis. Classic examples are placing fruit in a canteen at eye level, or pre-set selections and default choices. The latter are particularly effective. See Gabler Wirtschaftslexikon (2021), Nudging and Meszaros / Ho / Compagnucci (2022), Nudging Consent & the New Opt-Out System to the Processing of Health Data in England.

citizens have asserted their right to object.[20] There is a balancing act between individual data sovereignty and efficient healthcare provision. The more people who participate, the greater the individual and societal benefits of EHRs will be. Thus, it is always necessary to strike the right balance between individual data sovereignty and the goal of efficient healthcare provision.[21]

Discussion: The Commission proposal does not provide for a choice. EU citizens cannot prevent the secondary use of their electronic health records. While there is effective control in the case of primary use, this is lacking for secondary use because the Commission wants to significantly increase opportunities for health research and health policy in particular. Thus, electronic health records can be used for health research without the consent of the individual. This is mainly due to reasons of time and cost since obtaining the consent of every single EU citizen for various research projects, e.g. in the fight against cancer or rare diseases, would be very challenging. When balancing individual data sovereignty in this respect against efficient healthcare and research, such a solution is seen as preferable. In such cases, the Commission is aiming to ensure confidence and security with clear rules and prohibitions. A deterrent is provided principally by penalties. Nonetheless, a right to "opt-out" of the secondary use of one's own EHR should still be included. Even with such a right - as previously shown - a high number of "opt-outs" is unlikely and usage figures would increase significantly. At the same time, the individual retains freedom of choice. Thus, the goals of more efficient healthcare and research can be more effectively reconciled with individual sovereignty over one's own health data.

1.5 Wellness applications

In addition, the Commission proposal allows for health data generated by wellness applications to be fed into EHRs. Health data from wellness applications should also be capable of secondary use - including outside of the EHRs. The Commission has recognised that health data is increasingly being generated via fitness watches or fitness apps away from institutionalised healthcare.[22] The users of such applications have, among other things, the goal of maintaining a healthier lifestyle or want to specifically check and improve their state of health. On that basis, the Commission's proposal is understandable. However, it is important to bear in mind that the health data generated from wellness applications do not have the same quality and characteristics as those generated from institutionalised healthcare.[23] So, for example, users can also enter data themselves or the sensors of the devices might record incorrect health data.

The use of this data for individual healthcare and in scientific studies would be problematic if it proved to be (partially) incorrect. Therefore, all stakeholders, including manufacturers, users, health professionals and market surveillance authorities, have considerable responsibility for ensuring that this data can be put to good use.

With regard to secondary use, it is crucial that health data from self-certified wellness applications can be used without the explicit consent of users. Those concerned still have the freedom to decide whether they feed the data from wellness applications into their own EHRs. However, if this data is only used to independently check the individual's health status, the individual has no possibility of objecting to the secondary use of this data. The only option would then be to cease using the corresponding wellness application which cannot be a real solution. The Commission's proposal should certainly therefore be expanded to include a consent component for the secondary use of data from wellness applications.[24] This should take the form of an "opt-out". Comprehensive and comprehensible information for users in this regard is also necessary. Overall, there is still a need for a broad-based debate on the use of health data generated from wellness applications. The providers of these wellness applications not only have access to the health data generated, but can also combine it with other data, allowing sensitive information such as religious attitudes to be revealed.[25] There is therefore a need for comprehensive information for users, a broad-based public discussion and the possibility of an "opt-out". This may build confidence in the EHDS and the secondary use of data from wellness applications.

---

[20] Bertelsmann Stiftung (2022), Opt-out bei der Patientenakte. Die Möglichkeiten der Digitalisierung ausschöpfen, p. 3.

[21] See also ibid.

[22] This is not a European phenomenon but is apparent worldwide: The use of health apps in 2020 was 35% in Germany, 42% in the USA, 63% in India and 65% in China; see Acatech / Körber Stiftung / Universität Stuttgart (2022), Technik-Radar 2022: Was die Deutschen über Technik denken, p. 37.

[23] EDPB-EDPS (2022), EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space, p. 11.

[24] See also ibid., p. 12.

[25] Ibid., p. 11 et seq.

1.6 Anonymisation, pseudonymisation and synthetic data

The Commission's proposal also provides for health data to be made available, generally, in anonymised form - i.e. without reference to a person - and only exceptionally in pseudonymised form - i.e. personal data is processed in such a way that (ideally) it can no longer be assigned to a person without using additional information. It is important to remember that health data in anonymised form can only rarely be used for research purposes. Pseudonymised data is mainly required.[26]

Pseudonymisation can be carried out by various entities - be it the data holder or e.g. the access bodies. However, the Commission proposal does not explain exactly how the procedure for pseudonymisation will work - a number of technical procedures are conceivable.[27] As health data is very sensitive, it is right that only access bodies have the information to reverse pseudonymisation. This is also crucial in order to strengthen the confidence of EU citizens in the EHDS.

It should be noted, however, that pseudonymised health data can also, in principle, be traced back to an individual.[28] Thus a certain residual risk exists, not only for pseudonymised health data. Even with anonymised health data, the possibility of a person's identity being reconstructed cannot, in principle, be ruled out. This is particularly evident in the example of rare diseases as comparatively few people are affected and the cases are often very distinctive. Beyond this, there is also the possibility of reassigning health data to individuals by linking it to other information or by using new technological methods that are not currently conceivable.

In this respect, there is always a conflict of interests between allowing health research to be as accurate and efficient as possible on the one hand, and protecting individual health data on the other hand. The conflict itself cannot be resolved. It will always be necessary to examine each individual case and weigh up the conflicting interests using the instruments provided for in the Commission proposal - legally defined purposes for permitted secondary use, review of the facts within the framework of a data permit procedure and penalties. This is basically the right approach.

However, the Commission proposal should also promote the exchange of so-called synthetic data. This refers to data that is derived from original data and replaced by artificial data. Synthetic data aims to come as close as possible to the distribution characteristics of the original data[29],[30] without allowing the identification of the person on which it is based. Synthetic data is still not the perfect tool, however, because it cannot capture the whole truth.[31] Nevertheless, companies specialised in working with synthetic data are predicted to have significant growth potential.[32]

1.7 Ambitious timetable

Overall, the Commission proposal envisages an extremely ambitious timetable for the EHDS - in principle, the rules are set to take effect as early as twelve months after adoption of the Regulation (subject to the exceptions that postpone the start of its application by a further 1-3 years). The Commission aims to ensure that EU citizens gain access to and control over their health data as quickly as possible. In addition, the Commission wants to push ahead with preventive healthcare and research and create a single European market for health data. This is laudable but in the past other large-scale projects, such as the Medical Devices Regulation, have highlighted the difficulty of EU-wide implementation [see e.g. cep**Adhoc** Deadline extension for medical devices]. The EHDS is certainly no less complex. In this respect, the timetable is too ambitious - especially considering the fact that some Member States have immense catch-up potential when it comes to the digitalisation of their healthcare systems. The deadlines provided for in the Commission proposal should therefore be extended.

---

[26] Tschammler / Uecker (2022), Verordnungsentwurf zur Schaffung eines Europäischen Gesundheitsdatenraums – erster Überblick mit Fokus auf die Nutzung von Gesundheitsdaten für Forschungs- und Entwicklungsdaten, ZD-Aktuell, 01265.

[27] Drogkaris (2021), On overview of existing pseudonymisation techniques.

[28] Petri (2022), Die primäre und sekundäre Nutzung elektronischer Gesundheitsdaten. Zum Vorschlag der EU-Kommission für einen Europäischen Gesundheitsdatenraum, p. 418.

[29] Classical distribution characteristics of a frequency distribution are, for example, the mean, median, minimum or maximum values. If a certain mean value is found in the original data, the synthetic data should have the same mean value or come as close to it as possible.

[30] Drechsler / Jentzsch (2018), Synthetische Daten. Innovationspotential und gesellschaftliche Herausforderungen, p. 7.

[31] In concrete terms this means: A good data model is an important foundation for synthetic data because the relationships found in the original data are transferred to the synthetic data. See on this Drechsler / Jentzsch (2018), Synthetische Daten. Innovationspotential und gesellschaftliche Herausforderungen, p. 17. Accordingly, relationships that are missing in the original data cannot be detected in the synthetic data either. For more limitations of this method, see ibid., pp. 17-21.

[32] Der Spiegel (2022), Der erfundene Patient.

2 Legal Assessment

The Commission proposal is unproblematic with regard to competence, subsidiarity and proportionality vis-à-vis the Member States.

However, it should be noted that the proposal contains a plethora of delegations of power to the Commission - to adopt both delegated acts [see Art. 67] and implementing acts [in almost a third of the proposed provisions].

Delegations of power to adopt delegated acts [Art. 290 TFEU] are subject to the "concept of essential elements". This means that the "essential elements of an area (...)" are reserved for the legislator "and accordingly shall not be the subject of a delegation of power" [Art. 290 (1) TFEU].[33]

Two delegations of power to adopt delegated acts stand out in this case: The Commission will be empowered to amend (1) the list of "priority categories" of data for primary use and (2) the minimum categories of data for secondary use [Art. 5 (2) and Art. 33 (7)]. However, these are essential elements of the EHDS. The decision regarding the categories of data collected will determine the basic direction of European health data policy. This will ultimately define in concrete terms which - highly sensitive - health data will be collected by the EHDS for primary and secondary use.[34] This is a matter which must be determined by the European legislator - the legislator cannot delegate this decision on health data policy to the Commission. Thus, the delegations of power under Art. 5 (2) and Art. 33 (7) should be withdrawn.

D. Conclusion

The EHDS allows individuals to access and control their health data across the EU. This strengthens the fundamental freedoms of EU citizens in the area of cross-border healthcare. The EHDS aims to create a single market for health data, which can also be used to improve research, policy-making and regulatory activities. With digitalisation of health systems seeing very varied progress across the Member States, the EHDS may counteract further fragmentation, and now puts the onus on Member States to make real progress. A single market for health data will also allow for more competition in many areas of the health sector, e.g. with regard to the cross-border supply of medicines by pharmacies. However, the Commission's proposal needs to be improved in some areas, e.g. in the secondary use of health data, where those affected currently do not have sufficient control over their health data. Health data is, after all, very sensitive and worthy of protection, so EU citizens should be given the freedom to make decisions about such data. Overall, the EHDS - despite all the technicalities - is a necessary project in an increasingly digitalised world in which the EU and the Member States are in fierce competition with others.

[33] For detailed explanation see Eckhardt / Reichert (2022), Europe in the taxonomy trap, cep**Input** 2/2022, p. 9 et seq.

[34] Simply consider the dispute on whether data from wellness applications should become part of the EHDS; see for example EDPB-EDPS (2022), EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space, p. 12.